CASO ESTUDIO: SIMULACIÓN DE BRECHAS Y ATAQUES DE CIBERSEGURIDAD EN LA EMPRESA RANDOM S.A., BAJO UN ENTORNO DE LABORATORIO CONTROLADO

JORGE ANDRÉS RODRÍGUEZ CORTES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

CASO ESTUDIO: SIMULACIÓN DE BRECHAS Y ATAQUES DE CIBERSEGURIDAD EN LA EMPRESA RANDOM S.A., BAJO UN ENTORNO DE LABORATORIO CONTROLADO

JORGE ANDRÉS RODRÍGUEZ CORTES

Proyecto aplicado como requisito de grado para optar al título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director: Edilberto Bermúdez Penagos
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, octubre 2020

DEDICATORIA

Principalmente este trabajo está dedicado a Dios, porque él me ha dado el querer y el hacer por esta maravillosa profesión; además ha estado durante todo el proceso, sosteniéndome para no dejarme caer, acompañándome durante cada prueba, cruzando en mi camino personas valiosas y recursos que me han permitido adquirir conocimiento. Por todo esto y muchos más, Dios es el artífice de mis logros, porque no he sido yo, sino él obrando en mí.

También dedico este proyecto a mis padres, porque siempre me han apoyado y son el sustento de mi vida, en gran medida lo que soy y hasta donde he llegado, se lo debo a ellos. Gracias por todo su apoyo y amor incondicional, por alentarme a salir adelante, por creer en mí y recordarme que con dedicación, esfuerzo y disciplina se puede llegar muy lejos. También agradezco a mi familia en general, porque cada miembro ha sido importante durante este proceso, brindándome su ayuda incondicional y ánimo para no desfallecer hasta alcanzar mis metas.

AGRADECIMIENTOS

Todo el honor y toda la gloria son para Dios, porque ha sido inmensamente generoso en mi vida, otorgándome miles de bendiciones, guiando cada uno de mis pasos, corrigiéndome durante el camino y extendiendo su amor fraternal sobre mi familia, mi estudio y mi trabajo. A pesar de mis equivocaciones siempre he podido contar con su apoyo y tengo la completa certeza que él proveerá todo lo necesario conforme a su voluntad y su gracia.

Un especial reconocimiento y mi entera gratitud quiero ofrecer a mi director de proyecto, Ingeniero Edilberto Bermúdez Penagos, también a los asesores, Ingeniero Luis Fernando Zambrano Hernández e Ingeniero Alexander Larrahondo; en gran medida el desarrollo de este proyecto estuvo dirigido bajo sus sabios consejos y excelentes recomendaciones. Gracias a su compromiso y dedicación, este proyecto dejo varias experiencias y aportes positivos en mi vida.

A la Universidad Nacional Abierta y A Distancia, UNAD, por abrir sus puertas y demostrar que, si es posible hacer los sueños realidad, hoy al igual que el primer día de clases me siento orgulloso de ser parte de una de las mejores universidades a nivel nacional. A todas aquellas personas que de manera directa o indirecta han intervenido en el transcurso de mi vida, cada una de esas vivencias han permitido desarrollar mi carácter y aprender durante el proceso.

Jorge Andrés Rodríguez Cortes

CONTENIDO

pág.

INTRODUCCIÓN 23

1. DEFINICIÓN DEL PROBLEMA 24

1.1 ANTECEDENTES 24

1.2 DESCRIPCIÓN 26

1.3 FORMULACIÓN 27

2. JUSTIFICACIÓN 28

3. OBJETIVOS 29

3.1 OBJETIVO GENERAL 29

3.2 OBJETIVOS ESPECÍFICOS 29

4. MARCO REFERENCIAL 30

4.1 MARCO TEÓRICO 30

4.1.1 Seguridad Informática 31

4.1.2 Ataque informático 32

4.1.3 OSSTMM 38

4.1.4 MAGERIT 40

4.2 MARCO CONCEPTUAL 43

4.3 MARCO CONTEXTUAL 46

4.4 MARCO LEGAL 59

4.4.1 Ley 1273 de 2009 59

4.4.2 Ley 1581 de 2012 61

4.4.3 CONPES 3701 de 2011 62

4.4.4 CONPES 3854 de 2016 62

4.4.5 Ley 1928 de 24 de julio de 2018 62

5. DISEÑO METODOLÓGICO 63

5.1 METODOLOGÍA DE INVESTIGACIÓN APLICADA 63

5.2 TÉCNICAS APLICADAS 64

5.3 DESCRIPCIÓN DE LOS ESCENARIOS 65

5.3.1 Enfoque técnico 65

5.3.2 Enfoque administrativo 66

6. RESULTADOS Y DISCUSIÓN 67

6.1 IMPORTANCIA DE LA VIRTUALIZACIÓN 67

6.2 ENFOQUE TÉCNICO 68

6.2.1 Evaluación y análisis de riesgos 68

6.2.2 Pruebas de pentesting 77

6.3 ENFOQUE ADMINISTRATIVO 153

6.3.1 Diseño del plan estratégico de seguridad informática 153

6.3.2 Proyectos de seguridad Informática 184

7. CONCLUSIONES 191

8. RECOMENDACIONES 192

BIBLIOGRAFÍA 193

ANEXOS 199

LISTA DE TABLAS

pág.

Tabla 1.	Artículos de la ley de delitos informáticos 1273 de 2009	59
Tabla 2.	Degradación del valor	74
Tabla 3.	Probabilidad de ocurrencia	74
Tabla 4.	Valoración del impacto de las amenazas	74
Tabla 5.	Medidas para el tratamiento del riesgo	77
Tabla 6.	Riesgos inherentes del PESI	157
Tabla 7.	Costo general del diseño del PESI	159
Tabla 8.	Funciones de las áreas del departamento TI	161
Tabla 9.	Listado de videos para el enfoque técnico	199

LISTA DE CUADROS

pág.

Cuadro 1.	Identificación de los activos en la empresa RANDOM S.A.	69
Cuadro 2.	Valoración de los activos en RANDOM S.A.	72
Cuadro 3.	Identificación de amenazas en la empresa RANDOM S.A.	75
Cuadro 4.	Recursos necesarios para el laboratorio controlado	81
Cuadro 5.	Top de vulnerabilidades encontradas en el servidor de Bogotá	113
Cuadro 6.	Top de vulnerabilidades encontradas en el servidor de Cali	130
Cuadro 7.	Cronograma de actividades diseño del PESI	154
Cuadro 8.	Etapas y tiempo del plan estratégico de seguridad informática	155
Cuadro 9.	Valor total del talento humano	158
Cuadro 10.	Valor total de otros recursos	159
Cuadro 11.	Perfil del oficial de seguridad de la información	164
Cuadro 12.	Perfil del coordinador de seguridad informática	165
Cuadro 13.	Perfil del analista de seguridad informática	166
Cuadro 14.	Alcance del análisis de riesgos en la empresa RANDOM S.A.	172
Cuadro 15.	Identificación de los activos de información	173
Cuadro 16.	Amenazas y vulnerabilidades asociadas a los activos	175
Cuadro 17.	Valoración del riesgo	178
Cuadro 18.	Mapa de calor para la gestión del riesgo	180
Cuadro 19.	Tratamiento del riesgo	181

Cuadro 20. Modelo *AS* – *TO BE* de RANDOM S.A. 184

Cuadro 21. Cronograma de los proyectos de seguridad 189

Cuadro 22. Inversión económica de cada proyecto de seguridad 190

Cuadro 23. Playbook para un ataque de *Defacement* 200

Cuadro 24. Playbook para un ataque de *Ransomware* 203

LISTA DE FIGURAS

pág.

Figura 1. Porcentaje de vectores de ataque en diferentes países 25

Figura 2. Fases de un ataque informático 33

Figura 3. Fases de un pentesting basado en OSSTMM 39

Figura 4. Elementos relevantes en el análisis del riesgo 40

Figura 5. Gestión del riesgo de MAGERIT 42

Figura 6. Mapa geográfico de países infectados por Wannacry 48

Figura 7. Listado general de vulnerabilidades por año 49

Figura 8. Delitos informáticos que más afectan a los colombianos 50

Figura 9. Principales incidentes digitales reportados en 2019 51

Figura 10. Panorámica del cibercrimen en Colombia 52

Figura 11. Nivel de preparación ante un incidente digital 53

Figura 12. Prácticas de seguridad digital implementadas por las entidades 54

Figura 13. Porcentaje de cargos dedicados a la seguridad digital 55

Figura 14. Evaluación del riesgo cibernético 55

Figura 15. Porcentaje de empresas que identificaron incidentes digitales 56

Figura 16. Cambio en la gravedad de incidentes digitales 57

Figura 17. Gravedad de incidentes digitales 57

Figura 18. Presupuesto anual para la seguridad digital 58

Figura 19. Topología de la sede principal 65

Figura 20.	Dimensiones de valoración	71
Figura 21.	Criticidad	72
Figura 22.	Mapa de calor para la gestión del riesgo	76
Figura 23.	Fases de un pentesting basado en OSSTMM	78
Figura 24.	Topología del laboratorio	80
Figura 25.	Verificación inicial de la versión Kali Linux	82
Figura 26.	Actualización del archivo sources.list	82
Figura 27.	Ejecución de los comandos para actualizar Kali Linux	83
Figura 28.	Ejecución de los comandos para actualizar Kali Linux	83
Figura 29.	Verificación después de actualizar la versión Kali Linux	84
Figura 30.	Sitio oficial para descargar Metasploitable 2	84
Figura 31.	Configuración de la máquina virtual Metasploitable 2	85
Figura 32.	Configuración adicional para Metasploitable 2	85
Figura 33.	Resumen de la configuración para Metasploitable 2	86
Figura 34.	Banner de Metasploitable 2	86
Figura 35.	Mensaje de bienvenida de Metasploitable 2	87
Figura 36.	Escaneo de puertos filtrados por un firewall - escenario 1	87
Figura 37.	Escaneo de puertos abiertos con Nmap - escenario 1	88
Figura 38.	Escaneo de puertos con Zenmap - escenario 1	89
Figura 39.	Verificación de aplicaciones y versiones - escenario 1	89
Figura 40.	Script de Nmap para automatizar escaneo - escenario 1	90
Figura 41.	Script de Nmap para buscar vulnerabilidades - escenario 1	91
Figura 42.	Información sobre el módulo PHP 5.2.4	92

Figura 43.	Información sobre directorios del servidor web	92
Figura 44.	Escenario planteado para el primer escenario	93
Figura 45.	Página por defecto del servidor web	94
Figura 46.	Página principal similar a la de la empresa RANDOM S.A	94
Figura 47.	Acceso al módulo de PhpMyAdmin	95
Figura 48.	Ejecución del framework Metasploit	95
Figura 49.	Búsqueda del módulo CGI para ejecutar el ataque	96
Figura 50.	Información detallada del exploit php_cgi_arg_injection	96
Figura 51.	Búsqueda de payloads apropiados para el ataque CGI	97
Figura 52.	Configuración del exploit php_cgi_arg_injection	98
Figura 53.	Ejecución del exploit php_cgi_arg_injection	98
Figura 54.	Búsqueda de funciones para Meterpreter	98
Figura 55.	Captura de paquetes al realizar el ataque CGI	99
Figura 56.	Ejecución de comandos remotos en el servidor vulnerable	100
Figura 57.	Búsqueda del módulo CGI para ejecutar el ataque	101
Figura 58.	Modificación del archivo index.php	101
Figura 59.	Desfiguración parcial de la página web principal	102
Figura 60.	Descargar el código fuente original de la pagina	102
Figura 61.	Subir página web completamente modificada	103
Figura 62.	Desfiguración completa de la página web principal	104
Figura 63.	Creación de un usuario de bases de datos Mysql	104
Figura 64.	Ingreso al módulo de PhpMyAdmin	105
Figura 65.	Panel de administración de PhpMyAdmin con usuario creado	105

Figura 66.	Instalación de OpenVAS en Kali Linux	106
Figura 67.	Configuración automatizada de OpenVAS	106
Figura 68.	Verificación de servicios de OpenVAS	107
Figura 69.	Creación de un usuario administrador en OpenVAS	107
Figura 70.	Ejecución de OpenVAS	107
Figura 71.	Generación de la excepción en el navegador web	108
Figura 72.	Interfaz web de OpenVAS	108
Figura 73.	Panel de administración de OpenVAS	109
Figura 74.	Formulario para crear una tarea de análisis en OpenVAS	109
Figura 75.	Progreso del escaneo de vulnerabilidades	110
Figura 76.	Resultados del test de vulnerabilidades Servidor Bogotá	110
Figura 77.	Listado de vulnerabilidades detectadas del escenario I	111
Figura 78.	Información de OpenVAS sobre una vulnerabilidad	111
Figura 79.	Listado de vulnerabilidades encontradas en el servidor Bogotá	112
Figura 80.	Topología de red para la empresa RANDOM S.A. - Bogotá	115
Figura 81.	DMZ con un firewall de 3 interfaces	119
Figura 82.	DMZ con 2 firewall screened-subnet	120
Figura 83.	Tipo de cadenas establecida en IPTables	121
Figura 84.	Verificación de IPTables antes de ingresar las reglas	121
Figura 85.	Configuración del firewall IPTables en el servidor Bogotá	122
Figura 86.	Verificación de IPTables después de ingresar las reglas	122
Figura 87.	Escaneo de puertos escenario 1 sin resultado satisfactorio	123
Figura 88.	Ejecución del exploit escenario 1 sin resultado satisfactorio	123

Figura 89.	Información de maquina vulnerable Windows 7 X64 bits	124
Figura 90.	Programa para verificar vulnerabilidad Eternalblue	125
Figura 91.	Actualización para la vulnerabilidad Eternalblue	125
Figura 92.	Escaneo de puertos filtrados por un firewall	126
Figura 93.	Escaneo de puertos abiertos con Nmap – escenario 2	126
Figura 94.	Escaneo de puertos con Zenmap – escenario 2	127
Figura 95.	Script de Nmap para buscar vulnerabilidades – escenario 2	127
Figura 96.	Asistente de OpenVAS para iniciar un escaneo	128
Figura 97.	Representación gráfica de los resultados del test	128
Figura 98.	Listado de vulnerabilidades por aplicación	129
Figura 99.	Información de OpenVAS sobre una vulnerabilidad	129
Figura 100.	Topología planteada para el segundo escenario	131
Figura 101.	Firewall de Windows deshabilitado	131
Figura 102.	Búsqueda del módulo EternalBlue para ejecutar el ataque	132
Figura 103.	Información detallada del exploit smb_ms17_010_eternalblue	132
Figura 104.	Búsqueda de payload apropiados para el ataque EternalBlue	133
Figura 105.	Configuración del exploit smb_ms17_010_eternalblue	133
Figura 106.	Ejecución del exploit smb_ms17_010_eternalblue	134
Figura 107.	Búsqueda de funciones para Meterpreter	134
Figura 108.	Configuración del exploit smb_ms17_010_eternalblue	135
Figura 109.	Inicio de sesión en Windows 7	135
Figura 110.	Captura de la contraseña de inicio de sesión	136
Figura 111.	Identificación del proceso explorer.exe	136

Figura 112. Uso habitual de la maquina Windows 7 137
Figura 113. Captura de pulsaciones del teclado en Windows 7 137
Figura 114. Cámara web instalada en la maquina Windows 7 138
Figura 115. Captura de video de la cámara web en Windows 7 138
Figura 116. Establecer una sesión de video en Windows 7 139
Figura 117. Visualización de la sesión de video en la maquina Windows 7 139
Figura 118. Página principal del catálogo de Microsoft Update 142
Figura 119. Página de resultados para el parche KB4019264 142
Figura 120. Enlace de descarga de la actualización MS17-010 143
Figura 121. Búsqueda y confirmación de la actualización 143
Figura 122. Asistente de instalación del parche KB4019264 144
Figura 123. Progreso de la instalación del parche KB4019264 144
Figura 124. Terminación de la instalación del parche de seguridad 145
Figura 125. Configurando la actualización de Windows 7 145
Figura 126. Verificación de la actualización KB4019264 146
Figura 127. Verificación de la actualización KB4019264 146
Figura 128. Verificación de la actualización KB4019264 desde Metasploit 146
Figura 129. Topología de 6 host y un router protegidos por un UTM 147
Figura 130. Descargar la imagen ISO de Tails desde la página oficial 148
Figura 131. Configuración de la máquina virtual Tails 149
Figura 132. Ajuste del adaptador de red en la máquina virtual TAILS 149
Figura 133. Configuración predeterminada de la distribución Tails 150
Figura 134. Interfaz gráfica de TAILS e inicio del navegador TOR 150

Figura 135. Página principal de TAILS al ejecutar TOR 151
Figura 136. Visualización de URL tipo onion a través de DuckDuckGo 151
Figura 137. Acceso a la página de la Hidden Wiki 152
Figura 138. Búsqueda por el tópico ‘Hacker’ 152
Figura 139. Procesos de RANDOM S.A. 160
Figura 140. Organigrama de RANDOM S.A. 160
Figura 141. Estructura del comité de Seguridad Informática 162
Figura 142. Composición del comité de seguridad informática 163
Figura 143. Severidad de los riesgos identificados 181
Figura 144. Estructura del PESI 188

LISTA DE ANEXOS

pág.

ANEXO A. LISTADO DE VIDEOS 199

ANEXO B. PROCEDIMIENTO DE RESPUESTA ANTE INCIDENTES 199

CASO ESTUDIO: SIMULACIÓN DE BRECHAS Y ATAQUES DE CIBERSEGURIDAD EN LA EMPRESA RANDOM S.A., BAJO UN ENTORNO DE LABORATORIO CONTROLADO

GLOSARIO

SIMULACIÓN: Es un modelo abstracto de un sistema que permite evaluar el comportamiento y las características de un evento real. En informática, la simulación consiste en imitar una acción de un sistema, aplicación o servicio para validar su funcionamiento.

BRECHA DE SEGURIDAD: Se trata de una debilidad en un sistema informático que le permite a un atacante tener acceso no autorizado a datos digitales y en ocasiones destruir, eliminar, alterar, sustraer o transmitir información confidencial.

ATAQUE INFORMÁTICO: Es un actor malicioso con motivaciones lucrativas, ideológicas o terroristas que usa herramientas tecnológicas para afectar la confidencialidad, integridad y disponibilidad de la información.

CIBERSEGURIDAD: Área de la informática que se encarga de velar y proteger la privacidad de los datos digitales que se crean, almacenan y transmiten en una infraestructura tecnológica o sistema informático. En gran medida la ciberseguridad responsable de prevenir riesgos y contener incidentes de seguridad.

LABORATORIO: Es un ambiente controlado utilizado para realizar experimentos científicos, técnicos o tecnológicos. Este entorno está equipado con los recursos y medios necesarios para llevar a cabo pruebas, según el campo aplicación.

DEFACEMENT: Es un ataque informático dirigido a un sitio web que consiste en la modificación no autorizada del aspecto visual. Es ocasionado por un error de programación o fallo de seguridad en alguno de los componentes de la página web.

RANSOMWARE: Es un software malicioso que consiste en el secuestro o restricción de acceso a la información, mediante el cifrado no autorizado de los datos. Por lo general un atacante solicita el pago de un rescate a cambio de restablecer de retirar el cifrado.

SGSI: Sistema de Gestión de Seguridad de la Información, es el conjunto de políticas, procedimientos y procesos para la gestión eficiente del acceso, control y la seguridad de la información en una organización.

PLAN ESTRATÉGICO: Es el proceso organizado para el desarrollo de las actividades necesarias en la consecución de los objetivos de la organización. El plan estratégico brinda la dirección y los pasos que se deben tomar para el cumplimiento de los propósitos y metas establecidas por la alta gerencia de una empresa.

RESUMEN

El presente proyecto aplicado se basa en un caso estudio supuesto y es una aproximación técnica que busca recrear, bajo un ambiente controlado, 2 ataques informáticos que afectaron la triada de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) en la empresa RANDOM S.A. Con fundamento en esto, se busca analizar las vulnerabilidades en la infraestructura tecnológica, puntualmente en los servidores comprometidos, y proponer los controles necesarios que permitan asegurar los activos de la información en la organización.

El desarrollo del proyecto está basado en el uso de la metodología de la investigación aplicada, que permite a través del conocimiento práctico, proveer soluciones ante las amenazas informáticas identificadas en la organización, de manera complementaria, se utiliza la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) para realizar la evaluación del riesgo con el respectivo dictamen del estado actual de la seguridad de la información en la organización. También se aplica la metodología de *Ethical Hacking* OSSTMM (*Open Source Security Testing Methodology Manual*) que indica las etapas y actividades necesarios para realizar las pruebas de penetración de manera organizada y eficiente.

Palabras claves: Ataque informático, *Pentesting*, Seguridad ofensiva, Virtualización, Vector de ataque, Amenaza, Vulnerabilidad, Control informático, Política, Firewall, Riesgo tecnológico, Servidor, *Defacement*, *EternalBlue, Common Gateway Interface*, *Ransomware, Server Message Block, Wannacry*, Confidencialidad, Integridad, Disponibilidad, *Deep* Web, Virus informático, Metodología, Estrategia, Respuesta ante incidentes, Ciberseguridad.

INTRODUCCIÓN

Los ataques informáticos son una conducta delictiva que utiliza herramientas digitales relacionadas con las TIC (Tecnologías de la Información y las Comunicaciones) para llevar a cabo su cometido. Su principal objetivo es comprometer la información crítica, sensible y valiosa de organizaciones y personas alrededor del mundo. “En los últimos años se han evidenciado pérdidas multimillonarias relacionadas con el vertiginoso crecimiento de diferentes tipos y vectores de ataque, utilizados por los ciberdelincuentes para alterar la triada de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad)”[1].

Por lo tanto, es importante realizar una aproximación relacionada con ciberseguridad a través del proyecto aplicado de grado: “***Caso estudio: simulación de brechas y ataques de ciberseguridad en la empresa RANDOM S.A., bajo un entorno de laboratorio controlado***”. Este estudio permite analizar 2 ataques informáticos e identificar vulnerabilidades en sistemas operativos Windows y Linux, que están siendo simulados bajo el software de virtualización Virtual Box. Con base en este análisis se elaboran las estrategias pertinentes para prevenir la materialización de amenazas tecnológicas futuras.

La situación inicial parte de un enfoque técnico donde se presentan 2 incidentes de seguridad en diferentes sedes de la empresa RANDOM S.A; el primer ataque consiste en la desfiguración de la página web de la organización aprovechando una vulnerabilidad del lado del servidor web. En el segundo ataque se efectúa la extracción no autorizada de información de una base de datos alojada en una estación de trabajo con un sistema operativo desprotegido y desactualizado. Este proyecto se desarrolla usando un ambiente controlado, similar al entorno real; la finalidad es ejecutar pruebas de penetración y explotación de brechas de seguridad sin afectar directamente los activos de la información.

Adicionalmente, se cuenta con un enfoque administrativo, en el cual se plantea un proceso de restructuración del área TI (Tecnología de la Información), incluyendo la ampliación de su catálogo de servicios. Para que esto funcione apropiadamente, se requiere la vinculación de un consultor externo de seguridad de la información para el diseño, creación e implementación del PESI, (Plan Estratégico de Seguridad de la Información), y la definición de los riesgos tecnológicos más relevantes en la empresa RANDOM S.A.

[1] CISCO SYSTEMS. Reporte anual de Ciberseguridad, CISCO 2018. [En línea], febrero 2018 [Citado el 5 de noviembre de 2019]. Disponible en Internet: <https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf>

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES

Como soporte al planteamiento del problema y punto de partida del caso estudio, a continuación, se presentan tendencias y datos relevantes que evidencian los múltiples ataques informáticos hacia la infraestructura tecnológica en Colombia.

En la era digital ningún actor está exento de sufrir algún tipo de incidente informático, a causa de que diariamente las amenazas informáticas aumentan y evolucionan para adaptarse al medio, evitando así las medidas de protección. De acuerdo con una noticia del periódico el Tiempo, donde se entrevistó a Fabián Zambrano, director del centro de operaciones de seguridad de la empresa Digiware, "el volumen de ataques cibernéticos y el *malware* de difícil detección, son la amenaza con mayor índice de crecimiento"[2]. El diario líder en noticias de economía Portafolio[3], indica a través del balance de la Policía Nacional que el cibercrimen en Colombia aumenta paulatinamente; en el año 2018 se presentaron 21.687 denuncias sobre ataques informáticos, teniendo un incremento de 36% con respecto al año 2017 y en ese año se recibieron cerca de 11.618 denuncias relacionadas con delitos informáticos, presentando un incremento de 28.3% con respecto al año 2016.

El cibercrimen está compuesto por estructuras delictivas bien definidas que utilizan diferentes técnicas para suplantar la identidad digital de clientes, colaboradores y proveedores de las organizaciones con el fin de realizar una acción maliciosa como transferencias de dinero de manera no autorizada, difamación, daño en la reputación, suplantación, engaño, noticias falsas e incluso acciones activistas. El coronel Fredy Bautista, jefe de área del Centro Cibernético Policial, indica que: "los delitos informáticos son la segunda actividad ilegal que genera más rentabilidad a los delincuentes y se proyecta que para el año 2022 se presentan perdidas monetarias de hasta 8.000 millones de dólares"[4].

La compañía consultora EY mediante informe **¿La ciberseguridad es algo más que protección?**; indica que "Colombia es el país de América Latina con mayor

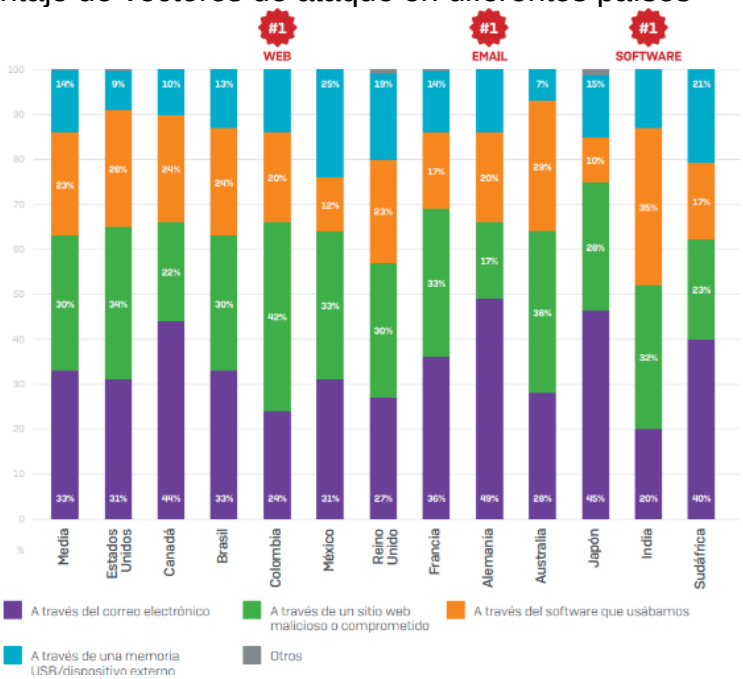
[2] EL TIEMPO. A diario se registran 542.465 ataques informáticos en Colombia. [En línea], 27 septiembre 2017 [Citado el 5 de noviembre de 2019]. Disponible en Internet: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370>.

[3] PORTAFOLIO. El secuestro de información desangra a las empresas del país. [En línea], 29 enero 2019 [Citado el 5 de noviembre de 2019]. Disponible en Internet: <https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729>.

[4] ENTER.CO. Colombia, el país con más ransomware en Latinoamérica, en 2018. [en línea], mayo 2019 [Citado el 5 de noviembre de 2019]. Disponible en Internet: <https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/>.

número de detecciones de *ransomware*, siendo Bogotá, Cali, Medellín, Barranquilla, Cartagena y Bucaramanga las ciudades con mayor cantidad de ataques informáticos a nivel nacional"[5]. Lo anterior es confirmado por el informe **El rompecabezas imposible de la ciberseguridad**, realizado por la empresa de soluciones de seguridad Sophos[6]. En la Figura 1 se observa que, durante el año 2018 Colombia fue el país que más recibió ciberataques a través de sitios web maliciosos.

Figura 1. Porcentaje de vectores de ataque en diferentes países



Fuente: SOPHOS. El rompecabezas imposible de la ciberseguridad. Resultados de una encuesta independiente patrocinada por Sophos a 3100 directores de TI. [En línea], junio 2019. Disponible en Internet: https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf, pág. 6.

En Colombia, el panorama de seguridad digital es incierto porque se presentan problemas significativos que a futuro pueden desencadenar en ciberataques de alto

[5] EY. ¿La ciberseguridad es algo más que protección? Encuesta global de seguridad de la información 2018-19. [En línea], 2019 [Citado el 5 de noviembre de 2019]. Disponible en Internet: <https://www.ey.com/Publication/vwLUAssets/EY-library-la-ciberseguridad-es-algo-mas-proteccion/%24File/EY-library-la-ciberseguridad-es-algo-mas-proteccion.pdf>.

[6] SOPHOS. El rompecabezas imposible de la ciberseguridad. Resultados de una encuesta independiente patrocinada por Sophos a 3100 directores de TI. [En línea], junio 2019 [Citado el 5 de noviembre de 2019]. Disponible en Internet: https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf, pág. 6.

impacto para las organizaciones, aunque, en comparación con otros países de la región, Colombia tiene un rango medio en cuanto a ciberseguridad, lo cual no es suficiente. La revista Semana[7] publicó una noticia relacionada con la posición que ocupa Colombia en materia de Ciberseguridad, en dicho artículo se menciona que la firma Comparitech, plataforma especializada en el análisis de servicios tecnológicos, realizó un estudio acerca de indicadores de ciberseguridad. En este análisis Colombia ocupa el puesto 39 de un total de 60 países analizados. En cuanto a la preparación para asumir un ciberataque Colombia obtuvo el valor de 0,56 sobre 1, lo que indica que el país está en una zona media y hace falta mejorar bastante en materia de ciberseguridad.

1.2 DESCRIPCIÓN

Las tecnologías de la información y las comunicaciones (TIC), son una poderosa herramienta que en la actualidad permiten interconectar a personas en todo el mundo, facilitando las relaciones interpersonales, el ocio y el intercambio cultural. En el ámbito corporativo las TIC facilitan los procesos misionales y optimizan las operaciones, lo que se traduce en ganancias y reducción en los tiempos de entrega de un servicio. La era actual gira en torno al procesamiento y trasmisión de datos en formato digital, las tecnologías modernas han permitido que las organizaciones sean más eficientes y productivas por medio procesos automatizados que soportan las metas del negocio. La digitalización de la información aumenta la eficiencia y operatividad en los entornos laborales, generando reducción en los tiempos de entrega de un bien, producto o servicio y un aumento significativo en las ganancias, además de promover el intercambio del conocimiento y agregar valor a las operaciones de una organización.

Para que lo anterior pase, los datos deben de trasmitirse por diferentes medios hasta llegar a los nodos donde las personas o sistemas tienen acceso para llevar a cabo un proceso y tomar decisiones. Después de esto, los datos deben ser retransmitidos, convirtiéndose en un ciclo continuo de intercambio de información. Ahora bien, para toda la información transmitida, es necesario garantizar que esta llegue correctamente, sin modificaciones y que sea íntegra, para lo cual existen diferentes técnicas, tácticas, procedimientos y herramientas para proteger la información. Con base en lo anterior, se puede decir que la ciberseguridad apoya desde varias capas la implementación de diferentes mecanismos que permiten salvaguardar los datos y fortalecer la triada de la seguridad de la información (Confidencialidad, Integridad y disponibilidad) en las organizaciones.

[7] SEMANA. Así está Colombia en el ranking de ciberseguridad mundial. [En línea], febrero 2019 [Citado el 5 de noviembre de 2019]. Disponible en Internet: <https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118>.

De manera análoga, la dependencia casi absoluta de las TIC se ha convertido en una de las principales preocupaciones para las organizaciones, siendo los ciberdelincuentes un factor inminente de amenaza que asecha los activos de la información corporativos; cada vez es más recurrente observar el vertiginoso crecimiento de ataques informáticos, siendo más sofisticados y ocasionado mayor impacto en las infraestructuras tecnológicas, además, los ciberdelincuentes pueden tener diferentes tipos de características y motivaciones para llevar a cabo un ataque informático.

En el ámbito informático y tecnológico, Colombia ha definido un sin número de leyes y normativas que guían la conducta de usuarios y profesionales que hacen uso de herramientas tecnológicas, además se han creado diferentes grupos especializados como el centro cibernético de la policía nacional, el CSIRT (*Computer Security Incident Response Team*) de diferentes entidades y ramas o COLCERT (Grupo de Respuesta a Emergencias Cibernéticas en Colombia) del ministerio de defensa; estos grupos de remediación y respuesta ante incidentes informáticos dedican diferentes esfuerzos y recursos en detectar e identificar actividades maliciosas que utilizan la tecnología para cometer un delito.

1.3 FORMULACIÓN

Dada la trascendencia, el valor y la importancia que tiene la información en los entornos corporativos, se ha evidenciado en los últimos años conductas delictivas que hacen uso de los recursos tecnológicos para afectar los pilares de la seguridad de la información y comprometer la información crítica, sensible y valiosa de las organizaciones. En temas de seguridad de la información, Colombia ha madurado considerablemente con respecto a años anteriores, hecho que se debe a las múltiples amenazas tecnológicas que se han presentado últimamente, sin embargo, el constante cambio tecnológico promueve que cada día se desarrollen nuevos vectores de ataque y aparezcan nuevas modalidades de cibercrimen. En ese sentido, las organizaciones deben estar preparados para afrontar la materialización de un ataque informático e identificar amenazas con el fin de aplicar las medidas necesarias antes de que ocurra un incidente de seguridad. Con base en esta premisa, se plantea la pregunta que será objeto de estudio:

¿Cuál es el impacto real que sufren las organizaciones frente a los ataques cibernéticos y qué alternativas de solución están implementando?

2. JUSTIFICACIÓN

En la actualidad, la información es uno de los activos más valiosos que poseen las organizaciones debido a que el ciberespacio gira en torno al procesamiento, almacenamiento y trasmisión de datos en formato digital. Las TIC (Tecnologías de la Información y las Comunicaciones), como eje central del ecosistema digital, han permitido tener acceso a diversas clases de contenidos y servicios interactivos que han favorecido el desarrollo de la sociedad, facilitando procesos, reduciendo los tiempos de respuesta y convirtiéndose en el puente de comunicación entre las personas y la información.

"Las TIC también han influenciado considerablemente el modo de vivir, la manera de pensar y la forma de interactuar de las personas, además, generan múltiples beneficios en áreas como la salud, educación, industria, agricultura, comercio, servicios, entretenimiento, empleo, entre otros"[8]. Sin embargo, la información y las comunicaciones están expuestas a una serie de eventos y riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información; esto se ve reflejado en degradación, perdida, modificación, generación, interceptación o compromiso total de los datos. Un claro ejemplo de riesgo es la materialización de ataques informáticos que amenazan el ciclo de la información e impactan negativamente al propietario de los datos.

Los ciberataques se han convertido es un problema mundial, el cual crece y evoluciona a la par con la tecnología, convirtiéndose en una de las principales preocupaciones de gerentes, directivos y personas en general. Como respuesta a esta preocupación surge la seguridad informática, siendo el área enfocada en la protección de los activos de la información y la infraestructura tecnológica por medio de técnicas, procedimientos, políticas y controles, aunque también se apoya en estándares, protocolos y metodologías. Como resultado de lo dicho previamente, se justifica la necesidad de ejecutar este proyecto aplicado con un enfoque técnico; para simular brechas digitales, pruebas de seguridad y análisis de vulnerabilidades. Adicionalmente se incluye un enfoque administrativo que permite evaluar el estado de la seguridad de la información en la organización por medio del análisis de riesgos y la generación de proyectos de seguridad informática. La finalidad de ambos enfoques es fortalecer la privacidad de los datos y proteger la infraestructura tecnológica de la empresa RANDOM S.A.

[8] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (ITU). Las TICS y la sociedad. [En línea]. [Citado el 30 de octubre de 2018]. Disponible en Internet: <https://www.itu.int/en/ITU-D/Digital-Inclusion/Indigenous-Peoples/PublishingImages/Las%20TIC%20y%20la%20Sociedad.pdf>.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Desarrollar pruebas de ataques informáticos encaminados hacia una mejora en la estrategia de ciberseguridad en la empresa RANDOM S.A por medio de la implementación de un PESI (Plan Estratégico de Seguridad de la Información).

3.2 OBJETIVOS ESPECÍFICOS

- Elaborar un análisis de riesgos bajo la metodología MAGERIT (Metodología de Análisis y gestión de Riesgos de Tecnologías de Información) a partir de las vulnerabilidades y amenazas encontradas en los activos de información comprometidos de la empresa RANDOM S.A.

- Realizar las pruebas de penetración de seguridad informática en los activos de información comprometidos de la empresa RANDOM S.A, con base en la metodología OSSTMM (Open Source Security Testing Methodology Manual).

- Diseñar un PESI (Plan Estratégico de Seguridad de la Información) para el fortalecimiento del modelo de seguridad de la empresa RANDOM S.A.

- Elaborar el catálogo de proyectos de seguridad informática para la organización RANDOM S.A., basado en los objetivos estratégicos del área TI.

4. MARCO REFERENCIAL

Al realizar la consulta de informes y documentos relacionadas con seguridad informática se puede encontrar múltiples trabajos académicos y textos que centran su objeto de estudio en ataques informáticos y ciberseguridad, sin embargo, no se aprecian investigaciones que se enfoquen puntualmente en el tipo de ataques que sufrió la empresa RANDOM S.A, por ende, basado en los referentes reconocidos se pretende elaborar este proyecto aplicado impregnado de cierto grado de innovación en cuanto a ataques de tipo CGI (*Common Gateway Interface*), *ransomware* y *EthernalBlue*.

En la actualidad se presenta un aumento de ataques distribuidos de denegación de servicio (DDoS), siendo la computación en la nube uno de los objetivos potenciales más apetecidos. “Con respecto a técnicas de cibercrimen, se destacan ataques de tipo *ransomware, phishing,* troyanos, *backdoors,* además, del uso de inteligencia artificial, *machine learning* y *Deep learning* enfocados al desarrollo de *malware*”[9]. Otra modalidad de cibercrimen es “el uso de criptomonedas para cometer actos delictivos y recibir el pago sin ser rastreado o ataques a sistemas ciberfísicos que controlan la operación de grandes emporios industriales como hidroeléctricas, sistemas de transporte entre otros”[10].

4.1 MARCO TEÓRICO

Con el auge de las tecnologías, los delitos han evolucionado por medio de técnicas y herramientas digitales que permiten llevar a cabo la actividad delictiva remotamente, ofreciendo practicidad, anonimato y un lucro bastante rentable. “Tales delitos informáticos van desde suplantar la identidad de una persona en Internet, ofrecer productos prohibidos por la red, adquirir contenido digital de manera ilegal, modificar la apariencia de un portal electrónico, uso de software no licenciado, e incluso, manipular infraestructura critica alterando su comportamiento y provocando un fallo en las operaciones de una organización”[11].

[9] OPTICAL NETWORKS. Tipos de ataques informáticos y previsiones para el 2019. [En línea], 2018. [Citado el 5 de noviembre de 2019]. Disponible en Internet: <https://www.optical.pe/tipos-de-ataques-informaticos-y-previsiones-para-el-2018/>.

[10] BENEDIKT, Luft. Los seis tipos de ciberataques para los que hay que prepararse en 2018. [En línea], enero 2018. [Citado el 12 de noviembre de 2018]. Disponible en Internet: <https://www.technologyreview.es/s/9908/los-seis-tipos-de-ciberataques-para-los-que-hay-que-prepararse-en-2018>.

[11] ACUARIO DEL PINO, Santiago. Delitos informáticos: generalidades. [En línea], 2018. [Citado el 12 de noviembre de 2018]. Disponible en Internet: <http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/599/1/Delitos%20Inform%C3%A1ticos.%20generalidades.pdf>, pág. 4.

4.1.1 Seguridad Informática . Es un campo especifico de las TIC (Tecnologías de la Información y la Comunicación) que "se encarga de proveer medidas, controles y aplicar herramientas tecnológicas con el objetivo de respaldar el cumplimiento de la triada de la información CID (Confidencialidad, Integridad y Disponibilidad) a nivel técnico"[12].

La información es uno de los activos más importantes y críticos para las organizaciones gracias al impacto e índice de penetración que tiene la tecnología en esta era digital, sin embargo, un mayor acceso a contenidos digitales implica mayores riesgos y es a partir de ese punto que la seguridad informática cobra relevancia porque permite prevenir y detectar vulnerabilidades potenciales a las cuales puede estar expuesta toda la información que se procesa de manera digital. Además, protege la infraestructura tecnológica a través de dispositivos y técnicas.

4.1.1.1 Principios de seguridad de la información. Un ataque informático busca afectar los principios de la seguridad de la información, mejor conocidos como la triada CID (Confidencialidad, Integridad y Disponibilidad). En MAGERIT[13], se describe brevemente las dimensiones de valoración para los pilares de la información y cómo un ataque informático puede afectarlos:

- **Integridad**: Atributo de la información que consiste en garantizar que no se ha modificado o alterado algún archivo de manera no autorizada o fuera de control. En términos del impacto, cómo se afectarían los procesos misionales si la información no es veraz y contundente. Se altera este pilar de la seguridad de la información cuando un atacante intercepta un mensaje y modifica su estructura o secuencia de bits.

- **Disponibilidad**: Propiedad de la información que garantiza el acceso de los usuarios y sistemas autorizados a un recurso computacional cuando así se requiera. En términos del impacto, cómo se afectaría la operación en la organización si un activo en particular es degradado o no se puede tener acceso a él. Se altera este pilar de la seguridad de la información cuando se crean múltiples peticiones a un servidor, con el objetivo de bloquear y dejar inaccesible un recurso.

[12] ESPAÑA. UNIVERSIDAD INTERNACIONAL DE VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme? [En línea], marzo 2018. [Citado el 13 de noviembre de 2018]. Disponible en Internet: <https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/ >.

[13] ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. [En línea], 2012. [Citado el 12 de noviembre de 2018]. Disponible en Internet: <https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html>, pág. 15.

- **Confidencialidad**: Característica de la información que consiste en la privacidad, es decir, que la información no se divulga a usuarios o procesos que no cuenten con el debido nivel de autorización. En términos del impacto, cómo se afectaría la imagen corporativa o la organización si la información crítica es accedida por un usuario sin el debido permiso. Se altera este pilar de la seguridad de la información cuando un ente no autorizado captura información que se transmite por la red de datos y puede visualizar su contenido.

4.1.2 Ataque informático. Dentro de la clasificación de delito en el ámbito tecnológico se encuentra el ataque informático o también conocido como ciberataque, que es toda actividad malintencionada que se lleva a cabo para afectar los pilares de la información (Confidencialidad, Integridad y Disponibilidad). Este tipo de ataques están dirigidos a plataformas e infraestructuras tecnológicas, siendo ejemplo de estas: redes de comunicación, aplicaciones web, bases de datos, sistemas informáticos, dispositivos de usuario final, servidores, etc.

La motivación de un delincuente informático varía dependiendo del objetivo y el entorno a atacar, por ejemplo, robo de información y espionaje corporativo, también puede ser de carácter ideológico, por entretenimiento, satisfacción personal o lucro financiero. “Los métodos de intrusión varían desde la explotación de brechas y debilidades en las configuraciones del recurso tecnológico hasta aprovechar descuidos y conductas humanas”[14]. Del mismo modo “se clasifica a los atacantes informáticos bajo una escala cuantitativa, (Nivel básico – Nivel medio – Nivel avanzado), dependiendo su nivel de conocimiento, experiencia y pericia”[15].

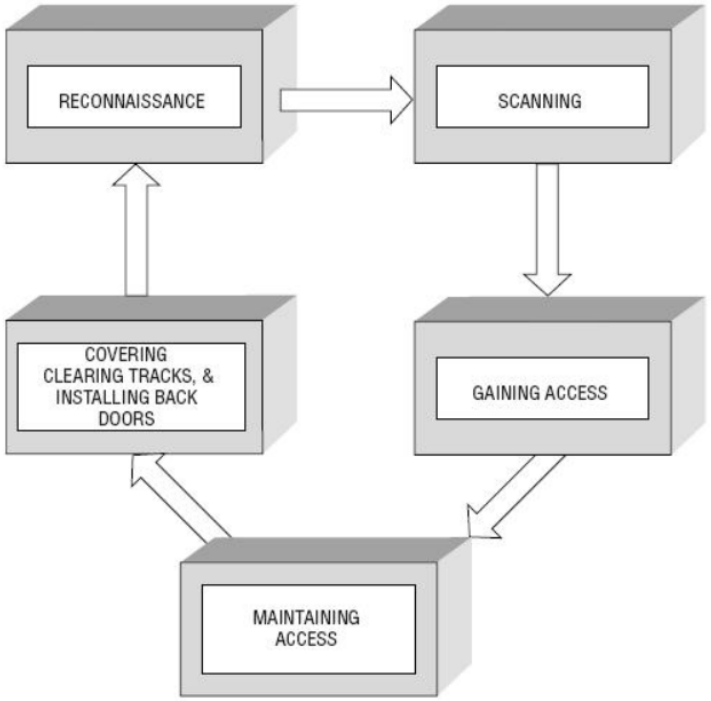
Los ataques informáticos han estado presentes desde hace varias décadas; con la masificación de Internet y el acceso a los contenidos digitales, personas inescrupulosas o curiosas se han dado a la tarea de desarrollar software malicioso que afecta a un sistema informático. Inicialmente los efectos de un ataque informático eran menores y se caracterizaban por su sencillez, sin embargo, con el paso del tiempo cada vez son más sofisticados y tienen como objetivo grandes organizaciones.

[14] SÁENZ, Pilar, Lecciones de un ataque informático. [En línea], mayo 2017. [Citado el 12 de noviembre de 2018]. Disponible en Internet: <https://razonpublica.com/index.php/economia-y-sociedad/10260-lecciones-de-un-ataque-inform%C3%A1tico.html>.

[15] ECUADOR. UNIVERSIDAD TÉCNICA DE COTOPAXI. Capítulo I, Aspectos generales de seguridad informática. [En línea], [Citado el 12 de noviembre de 2018]. Disponible en Internet: <http://repositorio.utc.edu.ec/bitstream/27000/536/1/T-UTC-1052%281%29.pdf>, pág. 21.

4.1.2.1 Fases de un ataque informático. Un ataque informático consiste en tomar ventaja de una vulnerabilidad para obtener algún beneficio, generar un comportamiento no deseado o impacto negativo sobre los activos de la información de una organización; "para llevar a cabo su cometido un ataque informático está divido en 5 fases"[16]. En la Figura 2 se aprecia la interacción y el flujo de cada etapa que compone un ataque informático.

Figura 2. Fases de un ataque informático



Fuente: PAHUJA, Surbhi. "Moral deviation: white hat reflecting the dark side". En: International Journal of Research in Management & Social Science. Disponible en Internet: < http://empyreal.co.in/downloads/ijrmss-volume-5-issue-1-january-march-2017.pdf >, pág. 15 - 19.

- **Reconocimiento (*Reconnaissance*)**: El atacante desarrolla una estrategia para obtener y analizar información del objetivo a atacar, en esta fase se puede utilizar técnicas tales como *Sniffing, Dumpter Diving* o la ingeniería social.

- **Exploración (*Scanning*)**: Con base en la información recolectada en la fase anterior, el atacante se dispone a detectar e identificar

[16] CASTRO, Ivette. Las 5 fases de un ataque informático. [En línea]. Septiembre 2018. [Citado el 21 de junio de 2019]. Disponible en Internet: <https://cerounosoftware.com.mx/2018/09/04/las-5-fases-de-un-ataque-informatico/>.

vulnerabilidades específicas, además de averiguar los puertos que la víctima tiene a la escucha para de este modo usarlos como acceso al sistema. En esta fase se utilizan herramientas automatizadas tales como analizadoras de puertos y escáner de red.

- **Obtener acceso (*Gaining Access*)**: El atacante explota las vulnerabilidades encontradas en la fase anterior y con esto obtiene acceso al sistema. La explotación puede darse de manera local, conectado desde la red de área local, LAN, o desde una red externa como Internet. En esta fase es común encontrar ataques como desbordamiento de Buffer, denegación de servicio (DoS), denegación distribuida de servicio (DDoS), filtrado de contraseña, fuerza bruta y robo de sesión.

- **Mantener el acceso (*Maintaining Access*)**: Al ganar acceso al sistema es necesario mantener un método alternativo de ingreso para volver acceder; por ende, se deben configurar herramientas o medidas que le permitan al atacante obtener el control de la maquina cuando así lo requiera sin necesidad de efectuar las fases anteriores. En esta fase se utilizan herramientas tales como *backdoors, rootkits* y troyanos informáticos.

- **Borrar las huellas (*Covering Tracks*)**: El atacante intenta destruir los posibles registros que lo vinculen con la intrusión en el sistema, por lo tanto, buscará eliminar los archivos log del sistema, de aplicación, de auditoria o de seguridad del recurso comprometido. Incluso evitar el envío de registros a herramientas centralizadas de recolección.

4.1.2.2 Clasificación de un ataque informático. Un ataque informático es toda actividad malintencionada que busca afectar negativamente un sistema informático o alguno de sus componentes, aprovechando una debilidad, por ejemplo: software malicioso, ingeniería social, infiltración en la red, explotación de vulnerabilidades y denegación de servicio. “La motivación de este tipo de conductas radica en obtener algún tipo de lucro económico, político, personal o activista”[17]. En la actualidad existen diferentes tipos de ataques informáticas, que dependiendo del método, objetivo y contexto se pueden clasificar en: “Monitoreo, Autenticación, Denegación de servicio, Interrupción, Interceptación, Modificación, Eliminación y Generación”[18].

[17] BELLO, Helena. Ciberseguridad: Tipos de ataques y en qué consisten. [En línea], julio 2020. [Citado el 12 de octubre 2020]. Disponible en Internet: <https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/ >.

[18] D’ADAMO Lucia. Qué es y en qué consiste un ataque informático. [En línea], octubre 2017. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://consulthink.it/es/que-es-y-en-que-consiste-un-ataque-informatico/>.

- **Interrupción**: Consiste en afectar la disponibilidad de un recurso computacional, retirándolo de circulación y dejándolo inaccesible para los sistemas, procesos o usuarios autorizados, por ejemplo, apagar un servidor para que no pueda recibir y/o contestar peticiones.

- **Interceptación**: Consiste en afectar la confidencialidad de un recurso computacional, esto sucede cuando un proceso, sistema o usuario no autorizado tiene acceso al contenido y no cuenta con el permiso correspondiente, por ejemplo, interceptar tráfico y manipular datos que circulan por la red.

- **Modificación**: Consiste en afectar la integridad de un recurso computacional, alterando el contenido y manipularlo para el beneficio propio, por ejemplo, modificar el contenido de los mensajes que se transmiten por la red.

- **Fabricación**: Consiste en afectar la autenticidad en un recurso computacional, creando objetos falsos e incluyéndolos sin autorización, por ejemplo, crear contenido falso y hacerlo pasar como legítimo.

4.1.2.3 Tipos de atacantes informáticos. Un atacante informático es un actor malicioso que adolece de principios éticos y su motivación es obtener un beneficio propio como la obtención de dinero, alguna ideología o por simple diversión. Se pueden clasificar en activos y pasivos según su manera de actuar, un atacante pasivo se centra en monitorizar y recopilar información sin afectar nada, en cambio un atacante activo tiene como objetivo degradar la información afectando la confidencialidad, integridad y disponibilidad.

- ***Black hacker***: Es un profesional capacitado en tecnologías de la información que, a pesar de poseer conocimientos sólidos, carece de ética y utiliza su saber para ingresar de forma no autorizada a sistemas, redes o información confidencial. Un hacker negro realiza pruebas de intrusión a sistemas y redes sin previa autorización y utiliza los hallazgos encontrados para su beneficio.

- ***Insider***: También conocido como intruso en la red, es un colaborador de la organización que produce un ataque informático desde el interior de la infraestructura tecnológica. Para llevar a cabo el ataque, se aprovecha del conocimiento de procedimientos, recursos y privilegios otorgados para el desempeño de una actividad en la organización.

- ***Script Kiddie***: Este tipo de atacante utiliza programas y herramientas que fueron desarrolladas por otros y se encuentran disponibles en internet, sin embargo, no sabe cómo utilizarlas de forma adecuada y no

posee los conocimientos técnicos. Su principal motivación es afectar un sistema de información por diversión o pasatiempo, sin medir las consecuencias de sus actos.

- ***Phreaker***: Es un atacante especializado en redes telefónicas conmutadas, capaz de obtener llamadas gratis o hacerlas en nombre de otra persona cargando el monto de las llamas a la factura de la víctima; también puede interceptar conversaciones a través de circuitos electrónicos.

- ***Carder***: Las tarjetas electrónicas son el foco de atención de este tipo de atacante, especialmente las tarjetas bancarias. Es capaz de falsificar tarjetas de crédito para realizar pagos en línea y cargar el cobro fraudulentamente a la cuenta de pago de una víctima.

- ***Newbie***: Novato o persona con falta de experiencia en el campo de la ciberseguridad que navega por internet buscando páginas y contenido relacionado con *hacking.* En ocasiones se utiliza este término despectivamente para referirse a principiantes.

- **Hacktivista**: Es un pirata informático que tiene motivaciones ideológicas y usa herramientas digitales para promover un movimiento no violento similar a la desobediencia civil. Entre las principales manifestaciones se encuentra la desfiguración de una página web, redirecciones a otros sitios, sabotaje digital, exposición de información confidencial y denegación de servicio.

4.1.2.4 Tipos de ataque Informáticos. Entre los ataques relacionados con el enfoque técnico se destacan los ataques hacia páginas web y la ejecución remota de comandos que permiten el secuestro de información privada. Este tipo de ataques es frecuente en entornos corporativos y ha crecido su número de casos en los últimos años.

Defacement: Este tipo de ataque aprovecha un fallo en la configuración, una mala práctica de programación o divulgación de información sensible para otorgar privilegios al código del sitio digital. “Una desfiguración de una página web consiste en modificar la apariencia sin autorización o permiso previo; por lo general este tipo de ataques son ejecutados por grupos hacktivistas con motivaciones ideológicas que buscan dejar un mensaje público de desobediencia civil”[19]. Las consecuencias de un *defacement* van

[19] UNIVERSIDAD DE LOS ANDES VENEZUELA, Deface, defacement, enmascaramiento y desfiguración. [En línea]. [Citado el 20 de noviembre de 2018]. Disponible en Internet: <http://blogs.ula.ve/seguridadtic/tag/defacement/>.

desde campañas de desprestigio, sanciones y multas que impactan directamente la imagen corporativa de la organización.

Un *Defacement* de una página web se determina por actividades que tienen como objetivo incluir algún fragmento de código malicioso para engañar al usuario final, comprometer el servidor y/o ejecutar una acción no deseada como suplantación, secuestro de sesión o capturar las pulsaciones de teclado de los visitantes. Vale la pena resaltar una de las principales causas de este tipo de ataque ocurre con la inyección de código cuando se insertan datos sospechosos e intencionalmente modificados en la aplicación web, como por ejemplo un comando o consulta. Estos datos hostiles pueden engañar al intérprete para que ejecute comandos o acciones no deseados, también se puede presentar acceso a los datos sin la autorización adecuada.

Ransomware: Software malicioso que encripta la información o impide acceso al sistema exigiendo un pago para tener nuevamente control sobre los archivos; en ocasiones a pesar de recibir el pago de la víctima el atacante deja inaccesible la información, ejemplo de este tipo de ataque es *Wannacry* o *Petya*. Este tipo de ataque cifra los archivos o unidades de almacenamiento de la víctima sin ninguna autorización, luego el ciberdelincuente exige un rescate a cambio de las llaves de descifrado. Este modelo de negocio es lucrativo y multimillonario, que apunta a cientos de miles de usuarios y organizaciones alrededor del mundo; recuperar el control sobre los equipos infectados con ransomware puede ser tedioso y llevar mucho tiempo. Las consecuencias de este ataque son: indisponibilidad de los datos, perdida de información crítica, sensible y valiosa, interrupción completa o parcial del negocio.

4.1.2.5 Pentesting. (Pruebas de penetración), se refiere a la práctica ejercida por un profesional de ciberseguridad en cuanto evaluaciones del estado de seguridad y protección de un sistema informático, se realizan por medio de un ataque cibernético que aprovecha vulnerabilidades para obtener acceso. El objetivo es descubrir fallos en la seguridad para de este modo generar las recomendaciones pertinentes en pro de prevenir ataques legítimos que sean generados por verdaderos ciberdelincuentes. Se pueden clasificar dependiendo el enfoque, es decir seguridad informática ofensiva o defensiva. El ejercicio de las pruebas de penetración debe estar bajo el consentimiento del propietario o administrador del sistema para que sea una actividad legal y autorizada, esto evita quebrantar algún tipo de ley, conforme a esto la documentación. Si se recibe información del objetivo a auditar, el test de intrusión se considera de caja blanca, pero, si el auditor no tiene ningún dato y parte de cero, la prueba se conoce como caja negra.

4.1.3 OSSTMM (Open Source Security Testing Methodology Manual). Es un estándar reconocido a nivel mundial desarrollado por el ISECOM[20] (*Institute for Security and Open Methodologies*) que se utiliza para realizar un análisis en profundidad sobre el nivel de seguridad de una organización, en esta metodología se propone realizar la evaluación de la seguridad de forma iterativa y secuencial. Fue publicado abiertamente en el año 2000, generando un hecho sin precedente debido a que en esa época no existía documentación pública para este tipo de actividades y actualmente se encuentra en la versión 3. A nivel de seguridad, la metodología OSSTMM divide los sistemas en dimensiones de la siguiente manera:

- Seguridad de la Información.
- Seguridad de los Procesos.
- Seguridad en las Tecnologías de Internet.
- Seguridad en las Comunicaciones.
- Seguridad Inalámbrica.
- Seguridad Física.

Además, se establecen fases para obtener resultados puntuales en cada una de las dimensiones de seguridad.

- **Búsqueda de vulnerabilidades**: Comprobaciones y pruebas automatizadas a un sistema o aplicación dentro de la red, su objetivo es identificar fallos existentes y posibles brechas que deben ser remediadas. Esa etapa va de la mano con los procesos de cacería de amenazas y recompensas por la detección de errores.

- **Escaneo de la Seguridad**: Detección de vulnerabilidades y análisis individual con base en la criticidad, tecnología y método de explotación, se realiza con herramientas especializadas. Existen soluciones y/o plataformas que realizan la validación de fallos de seguridad de manera automatizada y programable.

- **Test de Intrusión**: Pruebas de penetración para comprobar la seguridad del sistema, aplicaciones, también se utiliza para validar la maniobrar de un usuario y la respuesta ante in incidente de seguridad. Este tipo de ejercicios permite evaluar el estado de madurez en materia de ciberseguridad y la efectividad de los controles tecnológicos.

- **Evaluación del riesgo**: Análisis de seguridad desde la perspectiva el negocio, gobierno, leyes y el campo de acción de la organización. Es un

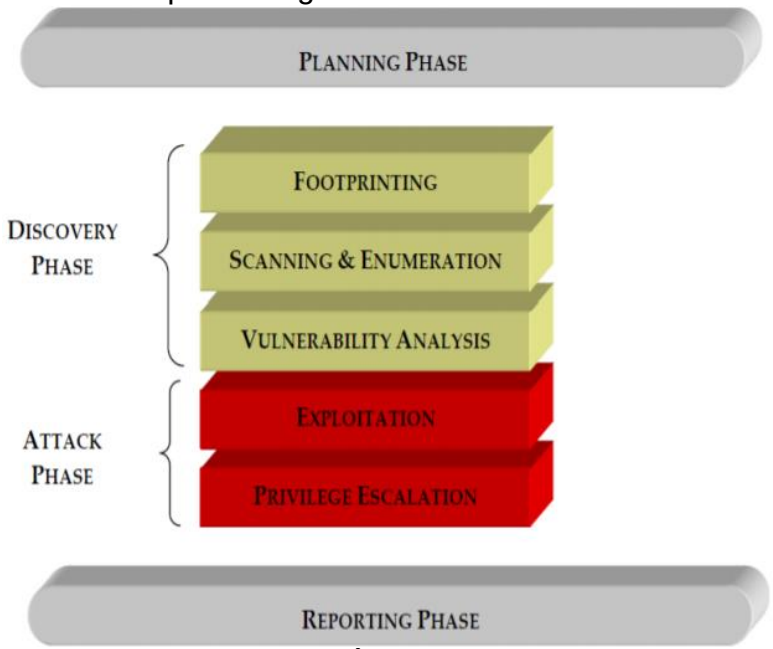
[20] ISECOM. Open Source Security Testing Methodology Manual (OSSTMM). [En línea], [Citado el 21 de noviembre de 2018]. Disponible en Internet: <http://www.isecom.org/research/>.

ítem indispensable para establecer el nivel de madurez en términos de seguridad, privacidad y protección de información. Esta fase es el insumo de la planeación estratégica y la continuidad del negocio.

- **Hacking Ético**: Simular el escenario en el cual un usuario ajeno al sistema tiene acceso y realiza acciones no autorizadas. Este tipo de simulaciones están supervisadas y autorizadas por la gerencia de la organización; su finalidad es realizar una Inspección profunda y recomendaciones para fortalecer la protección y seguridad de la información.

En la metodología OSSTMM se tienen en cuenta factores como la visibilidad, acceso, confianza, autenticación, confidencialidad, privacidad, autorización, integridad, seguridad y alarma, además se establecen etapas secuenciales que son Planeación, Descubrimiento, Ataque y Documentación. En la Figura 3 se observan las diferentes fases que componen un *pentesting* basado en OSSTMM.

Figura 3. Fases de un pentesting basado en OSSTMM

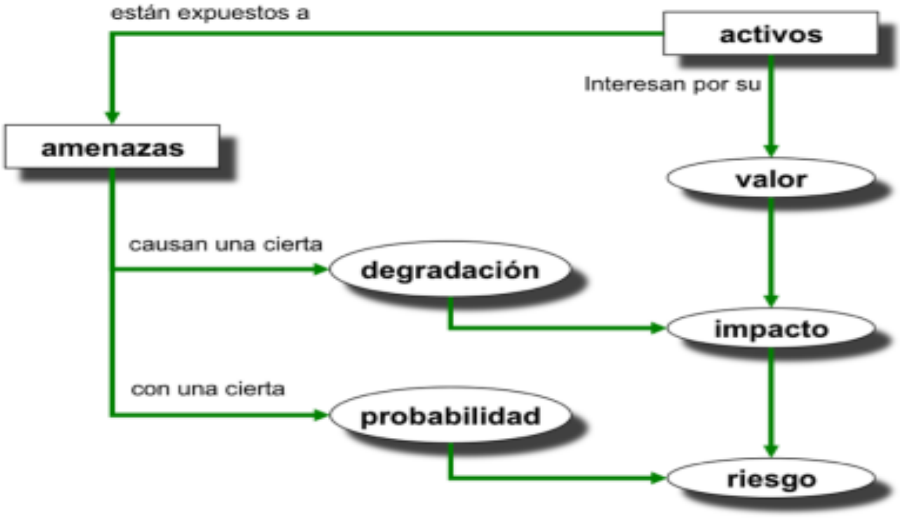


Fuente: ZULUAGA, Allen. Hacking Ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia. 2017. Trabajo de grado especialización en seguridad informática. [En línea], Disponible en Internet: <https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf>, pág. 39.

4.1.4 MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). Es una metodología desarrollada por el Consejo superior de Administración Electrónica en España, en la cual se presenta un conjunto de actividades, procedimientos y herramientas para elaborar el análisis y la gestión de riesgos tecnológicos en una organización, esto con "el principal objetivo de identificar posibles amenazas en la infraestructura tecnológica y afrontar los riesgos dependiendo su nivel de criticidad" [21].

MAGERIT es reconocida a nivel mundial porque permite realizar un análisis de riesgos tecnológicos completo, ordenado y de manera efectiva, considerando que cualquier activo de la información que tenga un valor considerable para la organización será identificado y clasificado para posteriormente asegurarlo sin dejar lugar a la malinterpretación o decisiones subjetivas por parte del evaluador. Para comprender MAGERIT, como la metodología más utilizada a nivel mundial para el análisis, evaluación y gestión de riesgos, es necesario comprender los conceptos clave, los cuales se presentan en la Figura 4.

Figura 4. Elementos relevantes en el análisis del riesgo



Fuente: ESPAÑA. PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I - Método. [En línea]. Disponible en Internet: < https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>.

[21] ESPAÑA. PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. [Citado el 21 de noviembre de 2018]. Disponible en Internet: < https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>.

- **Activo**: Elemento o entidad que componen un sistema informático, el cual cumple una función en particular y puede estar expuesto a incidentes que se traducen en consecuencias en los procesos críticos de la organización. Esta categoría incluye Información, servicios, Software, hardware, infraestructura tecnológica, locaciones físicas y cualquier tipo de recurso relacionado con TI (Tecnologías de la Información).

- **Dependencia**: Relación existente entre los activos de primer nivel que son esenciales, como la información y los servicios, y los activos de segundo nivel son los que apoyan y soportan a los de primer nivel. Cabe aclarar que los activos esenciales dependen directamente del resto de activos, esto quiere decir que de forma descendente se observa dependencia y de manera ascendente se aprecia como el impacto de la materialización de una amenaza en un activo de un nivel inferior afecta directamente al activo esencial.

- **Valor**: Es la medición que permite establecer el nivel de importancia de un activo, ya que cada activo es particular y necesita ser protegido acorde su naturaleza. Entre más valioso sea un activo requiere de mayor nivel de aseguramiento.

- **Amenaza**: Todo aquel acto o evento que de manera malintencionada o no, toma provecho de una vulnerabilidad para afectar, degradar o dañar un sistema informático o algunos de sus componentes.

- **Degradación**: Es la medida de la afectación o daño el cual puede verse reflejado en el valor de un activo.

- **Impacto**: Es la estimación que permite establecer el nivel de importancia o la prioridad con respecto al riesgo.

- **Probabilidad**: Cantidad posible de eventos sobre un activo de la información.

- **Riesgo**: Es la posible materialización de una amenaza aprovechando una vulnerabilidad en el sistema informático, se encuentra definido en función de la probabilidad y el impacto, para poder determinar su nivel y cómo tratarlo.

El análisis de riesgos es el estudio de las causas que pueden ocasionar eventos probables y no deseados con consecuencias negativas; esta actividad sirve para determinar el impacto y la probabilidad de una condición adversa mediante pasos secuenciales definidos en las siguientes etapas:

- Reconocer los activos de la información que son importantes para la operación, además de sus relaciones, respectivo valor y cómo afectaría su degradación o pérdida.

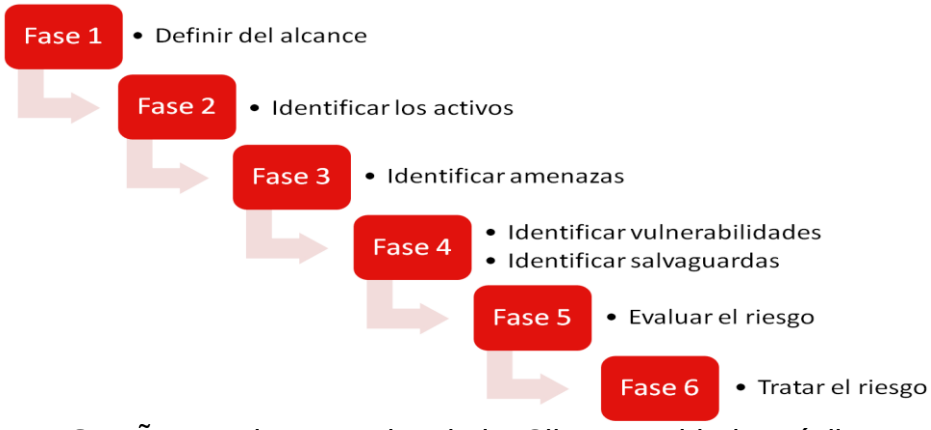
- Identificar las posibles amenazas y vulnerabilidades a las cuales pueden estar expuestos los activos de la información. Un activo puede tener múltiples amenazas y una amenaza puede afectar a varios activos.

- Proponer un conjunto de controles para los activos previamente identificados, establecer qué tan eficaces y eficientes son frente al riesgo de la materialización de una amenaza.

- Estimación (cuantitativa o cualitativa) del impacto que pueden generar las amenazas o posible efecto perjudicial sobre los activos. El impacto se define como la afectación causada sobre el activo generado por la materialización de la amenaza.

Para MAGERIT, la gestión de riesgos es un proceso estructurado de mejora continua que se establece en 2 etapas principales que permiten identificar activos, amenazas y controles basados en la probabilidad y el impacto que se traduce en la determinación del riesgo. “El análisis del riesgo les permite a las organizaciones asumir una postura firme ante el tratamiento del riesgo y de este modo garantizar la triada de la información (Confidencialidad – Integridad - Disponibilidad)”. En la Figura 5 se observa la estructura común para la gestión del riesgo.

Figura 5. Gestión del riesgo de MAGERIT



Fuente: ESPAÑA. Instituto Nacional de Ciberseguridad. ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. [En línea], 2017. [Citado el 25 de noviembre de 2018]. Disponible en Internet: < https://www.incibe.es/en/node/2789>.

MAGERIT propone como metodología de análisis de riesgos (MAR), las siguientes fases:

- **MAR.1**: Caracterización de los activos: Identificar los activos como elementos que componen el sistema, sus relaciones entre sí y definir el valor con base en su importancia dentro de la operación de la organización.

- **MAR.2**: Caracterización de las amenazas: Definir el contexto y entorno del sistema, considerando lo que puede pasar y el impacto derivado de la materialización de una amenaza.

- **MAR.3**: Caracterización de las salvaguardas: Identificar los elementos necesarios para proteger el sistema y conocer si se cuentan con medidas de seguridad acorde con la operación y procesos de la organización.

- **MAR.4**: Estimación del estado del riesgo: Tener una estimación de lo que puede ocurrir y de lo que probablemente ocurra. Con la ponderación es posible clasificar y organizar los riesgos según su probabilidad e impacto.

4.2 MARCO CONCEPTUAL

La información juega un rol imprescindible en el mundo, siendo el motor que hace girar los procesos en las organizaciones y cobra un factor relevante como uno de los activos más valiosos en el contexto empresarial. Con la adopción de tecnologías modernas, la información puede ser trasmitida en tiempo real gracias a Internet, favoreciendo el intercambio del conocimiento y agregando valor a las operaciones de las empresas.

A pesar de sus múltiples beneficios, Internet desde su concepción fue diseñada para ser eficazmente operativa, dejando de lado la seguridad, hecho que se ha visto reflejado en ataques informáticos con el objetivo de alterar o corromper la información transmitida. Otro aspecto relevante de Internet es que, para conseguir entregar sus servicios, la información se fragmenta en paquetes que son distribuidos por múltiples rutas, esto quiere decir que Internet es una red de redes, en la cual la administración y la seguridad de cada uno de sus nodos está sujeta al proveedor del servicio y a la normatividad vigente del país.

Los procesos críticos corporativos se encuentran en constante interacción con internet, por ende, los datos son transmitidos entre pares entrando en contacto con

redes inseguras que sobrepasan los límites de la legalidad; para el ICANN[22] (Corporación de Internet para la Asignación de Nombres y Números), la Deep Web, mejor conocida como web profunda, es la cara de internet que no se ve. En este ecosistema digital alterno se hacen publicaciones de sitios web con contenido prohibido o en algunas ocasiones ilegal, siendo esta la herramienta que utilizan los delincuentes para ofertar sus servicios, el principio de esta red es el anonimato y todo el contenido que allí se oferta no es indexado por los navegadores web.

En el ciberespacio en común encontrar amenazas que buscan aprovechar un fallo en la configuración para comprometer la confidencialidad, integridad y disponibilidad de un activo, generando degradación en la prestación de un servicio TI, esto se traduce en una debacle de la información almacenada o transmitida en un sistema informático. Los ataques informáticos cada día se especializan y son persistentes hasta el punto de explotar vulnerabilidades mediante *Exploit* y *Payload*.

> Exploit es un fragmento de código que se ejecuta para vulnerar algún sistema o aplicación en particular y de este modo tener control sobre una máquina. Este código ha sido desarrollado para aprovechar fallos en la configuración de un sistema, mejor conocido como vulnerabilidad, y de este modo obtener algún tipo de acceso a una maquina comprometida por el ataque. Un exploit es usado para acceder a un sistema utilizando una vulnerabilidad, y una vez adentro el atacante puede materializar el ataque[23].
>
> Payload se define como la carga útil o conjunto de acciones adicionales incluidas en el malware. Es también un fragmento de código que toma ventaja de una vulnerabilidad afectada por un exploit e inyecta código especializado para ejecutar una función en particular, permitiendo obtener control, acceso no autorizado, escalamiento de privilegios, denegación de servicio o alteración del comportamiento de la maquina comprometida" [24].

Existen herramientas que utilizan *exploit* automatizados para llevar a cabo una intrusión; en este aspecto vale la pena resaltar el reconocido entorno de *Metasploit*, "este *framework* de código abierto que se utiliza para el desarrollo y ejecución de *exploits*; esta herramienta sirve para llevar a cabo pruebas de penetración y auditorias de vulnerabilidades en sistemas informáticos, proporcionando la estructura y contenido de un amplio conjunto de librerías de *exploits* y *payloads*

[22] INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS- ICANN. The Dark Web: The Land of Hidden Services. [En línea], julio 2017. [Citado el 20 de noviembre de 2018]. Disponible en Internet: <https://www.icann.org/news/blog/the-dark-web-the-land-of-hidden-services>.

[23] EHACKING. ¿Qué es un exploit y cómo funciona? [En línea], enero 2020. [Citado el 12 de octubre de 2020]. Disponible en Internet: <https://blog.ehcgroup.io/2020/01/15/15/46/10/7677/que-es-un-exploit-y-como-funciona/hacking/ehacking/>.

[24] RIZALDO, Hector. Qué es un Payload. [En línea], octubre 2018. [Citado el 20 de noviembre de 2018]. Disponible en Internet: <https://openwebinars.net/blog/que-es-payload/>.

gracias al aporte de la comunidad"[25]. Su contraparte es el sistema operativo Metasploitable; el cual "es una distribución de Linux configurada intencionalmente con fallos de seguridad, diseñada para ejecutar pruebas de concepto y ataques informáticos bajo un ambiente controlado. Es utilizada para identificar vulnerabilidades y poder analizarlas sin tener preocupación de afectar un recurso en producción"[26]. *Metasploit* y *Metasploitable* le permiten a un profesional de ciberseguridad adquirir las competencias ofensivas necesarias para llevar a cabo un *ethical hacking* y ver un ataque informático desde la perspectiva de un atacante.

En el ámbito del *pentesting* existen múltiples plataformas y aplicaciones especializadas durante la fase de reconocimiento y explotación que son utilizadas en cada etapa de la auditoria de seguridad, entre las más reconocidas se puede mencionar Nmap y OpenVas, como un conjunto de herramientas que se utilizan para el análisis, detección y gestión de vulnerabilidades.

> Nmap es escáner de red y puertos utilizado a nivel mundial por los profesionales de seguridad informática, sirve para validar puertos, servicios y recolectar información de un equipo. Mediante el uso de scripts previamente configurados se puede proveer detección avanzada de vulnerabilidades adaptándose a las condiciones de la red con control de flujo y congestión. Comúnmente NMAP es usado para escanear y explorar redes, además permite conseguir información importante de los nodos que componen la red, como por ejemplo versión del sistema operativo, servicios a la escucha, puertos abiertos, vulnerabilidades [27].
>
> Openvas (Vulnerability Analysis), es un framework avanzado para ejecutar pruebas, análisis detección y gestión de vulnerabilidades. Para realizar el análisis compara las vulnerabilidades con el listado de la NIST (NVT). Esta herramienta integra un conjunto de utilidades de seguridad informática que permite escanear vulnerabilidades y realiza pruebas de ethical hacking para validar las configuraciones ante posibles brechas de seguridad en sistemas remotos[28].

Sin embargo, se han presentado casos donde se han utilizado las herramientas de *pentesting* con fines maliciosos, además cada vez se presentan situaciones donde los ciber delincuentes usan los marcos de trabajo de *hacking* para infectar dispositivos con software malicioso, generando ataques malintencionados con

---

[25] METASPLOIT. "Penetration Testing Software, Pen Testing Security, The world's most used penetration testing framework". [En línea], [Citado el 21 de noviembre de 2018]. Disponible en Internet: <https://www.metasploit.com/>.

[26] KATZ, Wouter. "Research Project 2: Metasploit-able Honeypots". [En línea]. [Citado el 13 de noviembre de 2018]. Disponible en Internet: <https://homepages.staff.os3.nl/~delaat/rp/2012-2013/p95/report.pdf>.

[27] Página official de NMAP. The Network Mapper - Free Security Scanner. [En línea], [Citado el 21 de noviembre de 2018]. Disponible en Internet: <https://nmap.org/>.

[28] Página official de OPENVAS. OpenVAS - Open Vulnerability Assessment System, The world's most advanced Open Source vulnerability scanner and manager. [En línea], [Citado el 21 de noviembre de 2018]. Disponible en Internet: <http://www.openvas.org/>.

propósitos de modificación, eliminación o lectura no autorizada, de tal modo que el *malware* evite los controles de seguridad, debido a que para los sistemas de protección y prevención es más difícil detectar este comportamiento inusual o sospechoso.

Por tal motivo, es pertinente establecer las medidas de seguridad que le agreguen protección en diferentes niveles a los activos de la información y permitan su correspondiente aseguramiento, por ejemplo, un Firewall es un elemento hardware o software que se encarga de hacer filtrado de paquetes acorde con un conjunto de reglas previamente definidas. En la actualidad los Firewall integran otras funcionalidades como antivirus, inspección profunda de paquetes, perfiles de seguridad basado en control web y por aplicación, canales cifrado de comunicación, enrutamiento, gestión de identidades, entre otros.

Otra herramienta de seguridad especializada es el IPS (*Intrusion Prevention System*), dispositivo o aplicación que analiza el comportamiento de un host o una red, su funcionamiento está basado en la heurística o una base de datos de firmas que al detectar alguna novedad o comportamiento inusual lo cataloga como sospechoso, además puede ejecutar acciones en tiempo real que permiten realizar el análisis e inspección del tráfico, con base en los resultados obtenidos toma decisiones y aplica políticas para proteger los activos de la información. Este tipo de soluciones permiten control sobre los *hosts* de la organización y ofrecen protección ante amenazas en tiempo real.

4.3 MARCO CONTEXTUAL

Con el avance de la tecnología los ataques informáticos han ido evolucionado exponencialmente pasando de simples archivos ejecutables con código malicioso, al uso de inteligencia artificial, aprendizaje profundo y amenazas persistentes. Lo anterior se ve reflejado en “tendencias de malware combinado como, por ejemplo, gusanos y *ransomware*, también el uso de tráfico cifrado como método para ocultar actividades malintencionadas, la complejidad de los ataques DDoS (*Distributed Denial of Service*) o el incremento de ciberamenazas hacia tecnologías IoT”[29].

Los ataques informáticos son una verdadera preocupación para las organizaciones privadas y públicas que soportan sus procesos operativos en las TIC (Tecnologías de la Información y la Comunicación). Este hecho es la principal causa de alarma debido a que se exponen al compromiso y degradación de la información crítica, sensible y valiosa. A continuación, se presentan datos relevantes que es importante

[29] CISCO SYSTEMS. Cisco 2018 Annual Cybersecurity Report. [En línea], 2018. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2>.

tener en cuenta durante el caso de estudio aplicado, esto se evidencia en el aumento de los ataques informáticos durante los últimos años en Latinoamérica, enfocándose en Colombia. Acorde con la empresa de seguridad ESET Latinoamérica, "en 2016 el 46.7% de las organizaciones en Colombia se vio afectada por algún tipo de incidente de seguridad relacionado con malware"[30], adicionalmente en ese mismo año se presenta el 56% de las organizaciones encuestadas con preocupación ante los códigos maliciosos, seguido de un 52% vulnerabilidades en el software y sistemas, 32% *ransomware* y 27% *Pishing*.

En cuanto a código malicioso se refiere, "el *ransomware* se posicionó en segundo lugar con el 16% superando al *Pishing* con 15%"[31]. Otro hecho relevante sobre ataques cibernéticos lo menciona la revista Portafolio[32], con base en el informe realizado por Digiware; en Colombia para el año 2017 se generaron 198 millones ataques informáticos, lo que en promedio seria 542.465 ciberataques a diario, siendo el sector financiero el principal afectado con un 39,56% (214.600 casos), seguido por las telecomunicaciones con 25,5% (138.329 casos), el gubernamental con 15,4% (83.756 casos) y la industria con 9,4% (51.263 casos).

La revista Semana[33] menciona cifras de la DIJIN para el año 2017, donde los delitos informáticos en Colombia aumentaron 28.3%; la población civil, el sector financiero, educación y gobierno son los más afectados, esto permite identificar los principales objetivos que son críticos para el desarrollo sostenible de una nación. Por otro lado, la Fiscalía General de la nación declaro que "en 2017 el delito informático ha crecido considerablemente con respecto a otro tipo de modalidades delictivas, abriendo más de 8.682 investigaciones por esta conducta"[34].

---

[30] ESET LATINOAMÉRICA. ESET Security Report Latinoamérica 2017. [En línea], 2017. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf>, pág. 10.

[31] ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS (ACIS). Un 46.7% de empresas en Colombia sufrió algún incidente de seguridad informática el último año. [En línea], 2017. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <http://acis.org.co/portal/content/un-467-de-empresas-en-colombia-sufri%C3%B3-alg%C3%BAn-incidente-de-seguridad-inform%C3%A1tica-el-%C3%BAltimo-a%C3%B1o>.

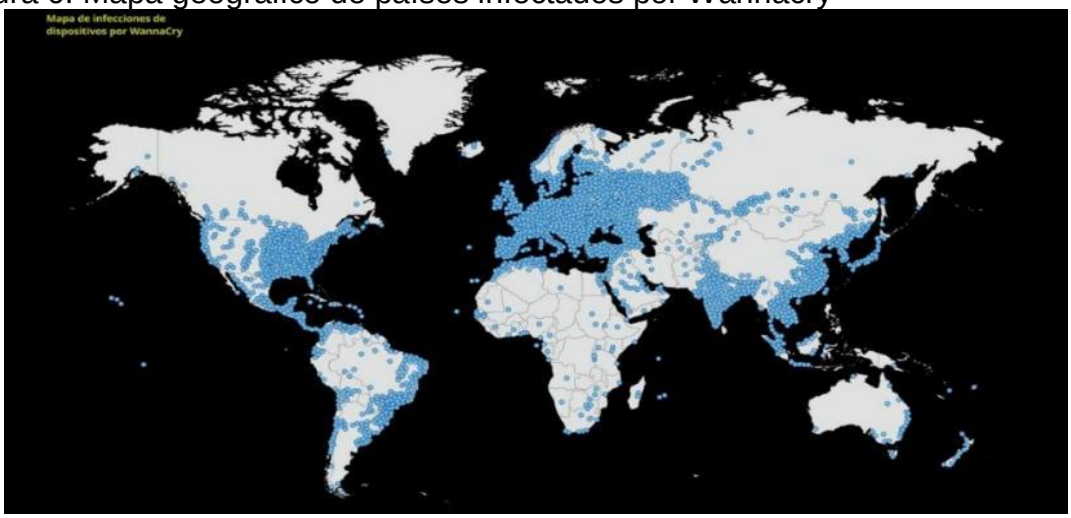
[32] PORTAFOLIO. Colombia registró 198 millones de ataques cibernéticos en el 2017. [En línea], septiembre 2017. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://www.portafolio.co/tendencias/colombia-es-uno-de-los-paises-mas-afectados-por-ataques-ciberneticos-510128>.

[33] CARREÑO, Itzel. El cibercrimen aumentó 28% en Colombia durante 2017, siendo los ciudadanos los más afectados. [En línea]. 2017. [Citado el 28 de noviembre de 2018]. Disponible en Internet: <https://www.mediatelecom.com.mx/2017/12/29/el-cibercrimen-aumento-28-en-colombia-durante-2017-siendo-los-ciudadanos-los-mas-afectados/>.

[34] SEMANA. El cibercrimen en 2017: la amenaza crece sobre Colombia. [En línea]. 2018. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979>.

Una de las principales amenazas informáticas son las aplicaciones maliciosas que cifran la información, por ejemplo: “En 2017 se hizo público el ataque de ransomware *Wannacry*, el cual afectó aproximadamente 200.000 equipos alrededor del mundo en 150 países, en Colombia se presentaron 52 víctimas según datos de la policía nacional”[35], en la Figura 6 se observa el mapa donde se resaltan los sitios geográficos donde se ejecutó el ataque informático, afectando principalmente a versiones del sistema operativo Windows 7.

Figura 6. Mapa geográfico de países infectados por Wannacry



Fuente: EL CONFIDENCIAL. Tras la sangría de 200 M de WannaCry, esta es la factura que nos dejará Petya. [En línea], Julio 2017. Disponible en Internet: <https://www.elconfidencial.com/tecnologia/2017-07-18/wannacry-petya-notpetya-deloitte-bra_1408510/>.

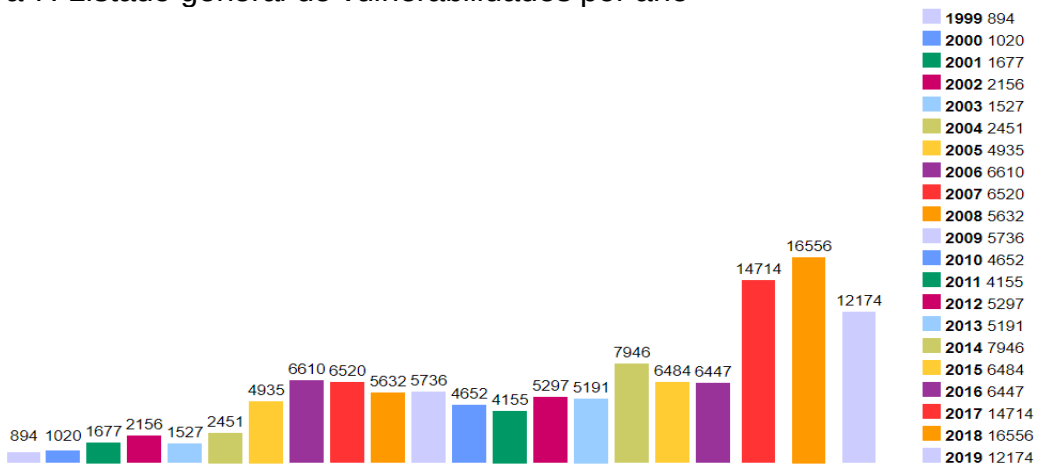
El periódico el Tiempo[36], señalo que el año 2017 batió un record histórico de vulnerabilidades, con base en el listado *Common Vulnerabilities and Exposures* (CVE) donde se publican abiertamente las vulnerabilidades para numerosos productos y servicios. El identificador CVE es una nomenclatura estándar la cual permite identificar un fallo de seguridad para un producto o tecnología, esta información es utilizada para describir una vulnerabilidad y recomendar medidas de mitigación, además se encuentra consignada en una base de datos que está disponible públicamente.

[35] EL CONFIDENCIAL. Tras la sangría de 200 M de WannaCry, esta es la factura que nos dejará Petya. [En línea], Julio 2017. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://www.elconfidencial.com/tecnologia/2017-07-18/wannacry-petya-notpetya-deloitte-bra_1408510/>.

[36] EL TIEMPO. En 2017 se reportaron más de 14.600 vulnerabilidades informáticas. [En línea], 2018. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-vulnerabilidades-informaticas-registradas-en-2017-171214>.

En el año 2017 se presentaron 14.714 vulnerabilidades, en el año 2018 se reportaron 16.556 vulnerabilidades, siendo este el año con más casos notificados hasta la fecha. En el año 2019 se registraron 12.174 brechas de seguridad para diferentes fabricantes de tecnología, lo que muestra que en los últimos 3 años las vulnerabilidades han crecido exponencialmente en comparación con años anteriores, evidenciando una alarmante situación. En la Figura 7, se presentan los datos estadísticos de las principales vulnerabilidades por año del listado CVE[37].

Figura 7. Listado general de vulnerabilidades por año



Fuente: CVE DETAILS. Browse Vulnerabilities by date. [En línea]. Disponible en Internet: <https://www.cvedetails.com/browse-by-date.php>.

La ciberseguridad en Colombia se encuentra en estado de alarma temprana, porque a pesar de la normatividad vigente y de los esfuerzos de entes encargados y especializados en proteger la información de los colombianos; las amenazas informáticas están presentes esperando la oportunidad para aprovechar una vulnerabilidad y tomar control del activo más preciado en esta era digital, la información. La seguridad de la información se ha convertido en una preocupación para las organizaciones, por ende, los profesionales de ciberseguridad deben estar actualizados sobre técnicas, tácticas y procedimientos que permitan mantener la integridad y confidencialidad de la información que se procese y/o transmita desde y hacia la organización.

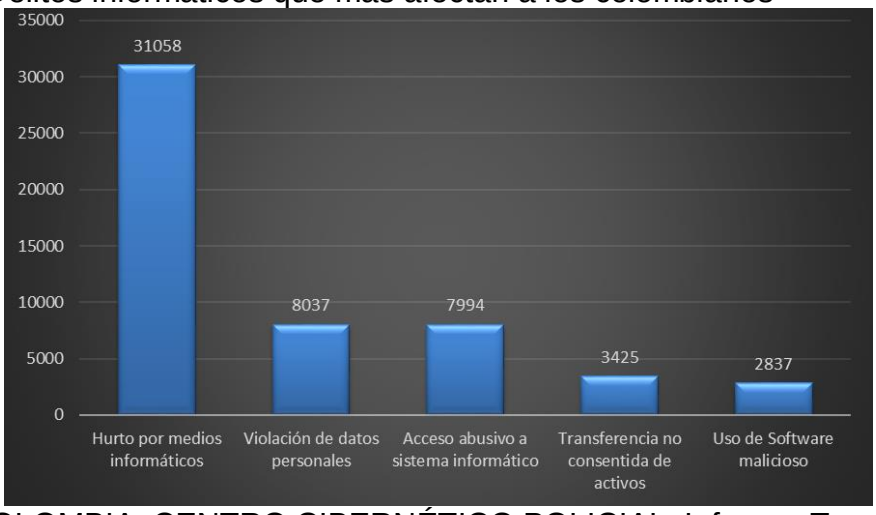
Por lo anterior, la ciberseguridad es un campo de acción que crece de manera exponencial y debe analizarse con sumo detalle, de cara a afrontar nuevos desafíos y proponer soluciones ante las diferentes problemáticas y modalidades de ciberdelincuencia que día a día se hace más evidentes en la sociedad.

[37] CVE DETAILS. Browse Vulnerabilities by date. [En línea]. [Citado el 19 de noviembre de 2019]. Disponible en Internet: <https://www.cvedetails.com/browse-by-date.php>.

De acuerdo con el informe de **Tendencias del cibercrimen en Colombia 2019 – 2020**, realizado por el centro cibernético de la Policía Nacional[38], -en colaboración con otras organizaciones estatales-, este documento está basado en la estadística de la plataforma de atención a incidentes informáticos. Se evidencia que el cibercrimen en Colombia ha generado pérdidas cercanas a 300 a 5000 millones de pesos COP, dependiendo el tamaño de la empresa. Lo anterior demuestra que la principal motivación del cibercrimen es el interés económico y la monetización de las ganancias generadas por los incidentes de ciberseguridad.

Es realmente preocupante observar el panorama de seguridad informática en Colombia donde "se presentaron 31058 casos relacionados con hurto por medios informáticos, 8037 eventos relacionados con violación de datos personales, 7994 reportes de acceso abusivo a sistema informático, 3425 transferencias no consentidas de activos y 2837 denuncias con uso de software malicioso"[39]. Para el año 2019, se presentó un aumento de 54% de incidentes, con respecto al año anterior, en la Figura 8 se muestran los principales delitos que impactan a la sociedad colombiana.

Figura 8. Delitos informáticos que más afectan a los colombianos



Fuente: COLOMBIA. CENTRO CIBERNÉTICO POLICIAL. Informe: Tendencias del cibercrimen en Colombia 2019 - 2020. [En línea], octubre 2019. Disponible en Internet:<https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf>, pág. 8.

[38] COLOMBIA. CENTRO CIBERNÉTICO POLICIAL. Informe: Tendencias del cibercrimen en Colombia 2019 - 2020. [En línea], octubre 2019. Disponible en Internet:<https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf>.

[39] Ibíd., pág. 8.

Los incidentes más reportados en Colombia siguen siendo los casos de tipo "*Phishing* con 42%, la suplantación de identidad con 28%, el envío de malware con el 14% y los fraudes en medios de pago en línea con 16%"[40]. En la Figura 9 se presenta el porcentaje y tipo de incidentes reportados durante el año 2019

Figura 9. Principales incidentes digitales reportados en 2019

Fuente: COLOMBIA. CENTRO CIBERNÉTICO POLICIAL. Informe: Tendencias del cibercrimen en Colombia 2019 - 2020. [En línea], octubre 2019. Disponible en Internet:<https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf>, pág. 9.

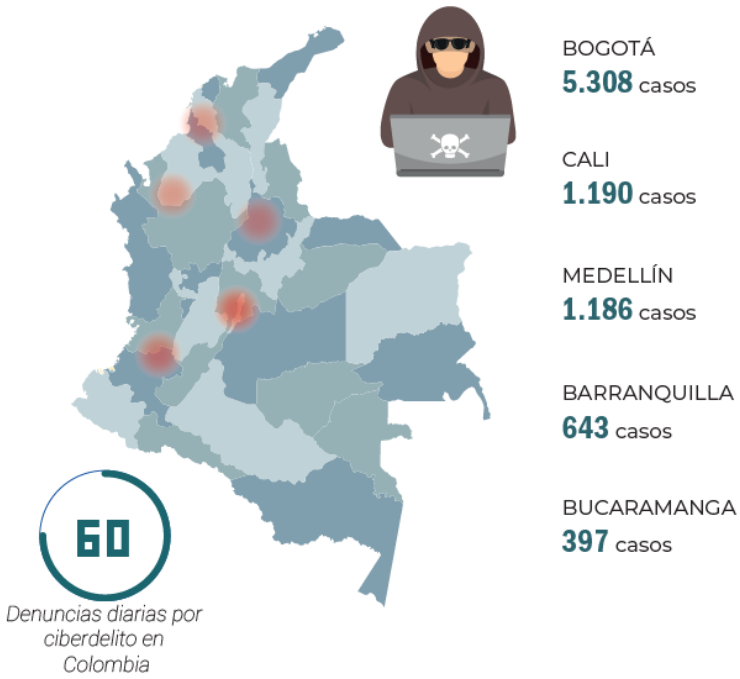
Es evidente que los ciberdelincuentes están evolucionando con el paso de la tecnología y día a día las técnicas utilizadas son cada vez más sofisticadas, evidenciado un claro incremento de ataques de malware y APT (Amenazas Persistentes Avanzadas), que se difunde por la red. Vale la pena resaltar que se han identificado nuevos métodos de propagación donde el software malicioso es dirigido a objetivos potencialmente atractivos para un atacante y ha dejado de ser cuestión al azar, adicionalmente el ransomware es una modalidad emergente que se ha convertido en una de las principales preocupaciones a nivel mundial, por lo que la prevención es un factor clave para identificar posibles amenazas y erradicarlas antes de su materialización.

Otro aspecto a tener en cuenta más allá de lo técnico, es el factor humano, siendo el eslabón más débil cuando se trata de seguridad de la información. En este aspecto la sensibilización en cuanto a tecnologías de la información y las comunicaciones, es un punto clave para que una estrategia de prevención y protección sea efectiva; personal consciente de los peligros digitales acompañado de salvaguardas adecuados reduce considerablemente la superficie de un ataque informático y previene posibles compromisos de los activos de la información

[40] Ibíd., pág. 9.

Se ha identificado que las ciudades con mayor número de denuncias relacionadas con delitos informáticos son: “Bogotá con 5308 casos, seguido por Cali con 1190, Medellín con 1186, Barranquilla con 643 y finaliza Bucaramanga con 397 casos reportados” [41]. De lo anterior se destaca que las principales ciudades de nuestro país son el objetivo de los ataques informáticos, debido a que estas ciudades son las que cuentan con mayor número de habitantes y acceso a internet, en la Figura 10 se presenta el mapa de calor del delito informático en Colombia.

Figura 10. Panorámica del cibercrimen en Colombia



Fuente: COLOMBIA. CENTRO CIBERNÉTICO POLICIAL. Informe: Tendencias del cibercrimen en Colombia 2019 - 2020. [En línea], octubre 2019. Disponible en Internet:<https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf>, pág. 10.

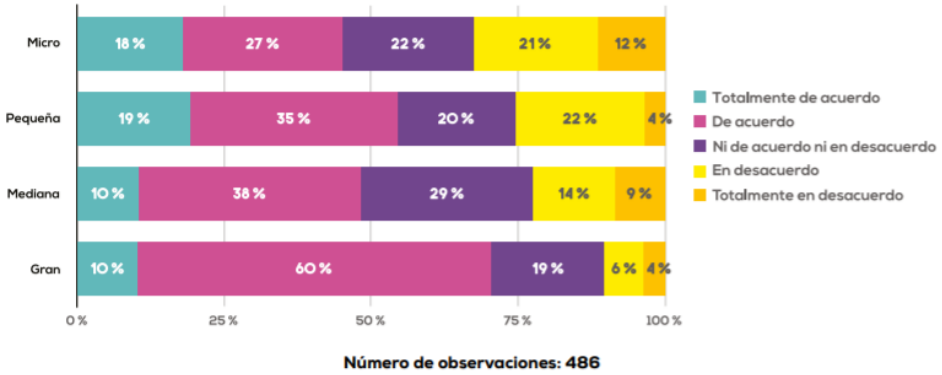
Es importante recalcar que la adopción de las TIC en las ciudades capitales del territorio nacional conlleva que usuarios legítimos y atacantes convivan en el mismo ciberespacio, lo cual es un riesgo inherente que debe ser asumido con responsabilidad, de tal modo que cada actor de este escenario conozca sus derechos y deberes. En internet abunda la información de acceso libre y este hecho es aprovechado por los atacantes informáticos para distribuir software malicioso en cualquiera de sus modalidades.

[41] Ibíd., pág. 10.

Para contextualizar la situación actual de la seguridad de la información en las organizaciones, se presentan datos estadísticos del informe **Impacto de los incidentes de seguridad digital en Colombia 2017**, realizado por el Banco Interamericano de Desarrollo (BID), el ministerio de las tecnologías de la información y las comunicaciones (MINTIC) y la Organización de los Estados Americanos (OEA)[42]. Este estudio se realizó entre el mes de agosto de 2016 y el mismo mes del año 2017 a 583 entidades estatales de orden nacional y a 515 empresas privadas de diferentes sectores y tamaños. El objetivo de este informe era evaluar el estado actual de la seguridad digital a nivel gubernamental y corporativo. A continuación, se presentan algunos de los resultados relevantes que están intrínsecamente relacionados con la naturaleza del presente proyecto.

En la Figura 11 se observa claramente que de un total de "486 empresas encuestadas, entre más grande sea la empresa, el nivel de preparación ante un incidente digital es mayor"[43]. Esto indica que las grandes empresas comprenden y son conscientes del valor agregado y el retorno a la inversión en materia de ciberseguridad.

Figura 11. Nivel de preparación ante un incidente digital



Fuente: BID, MINTIC, OEA. Estudio de Seguridad digital en Colombia. [En línea], 2017. Disponible en Internet: <http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf>, pág. 40.

A nivel de prácticas implementadas para garantizar la seguridad digital en las organizaciones se definieron políticas, medidas, técnicas y normas las cuales están alineadas con estándares internacionales. En el aspecto organizacional se definen los roles y departamentos dedicados a ciberseguridad; en cuanto a políticas se cuentan con directrices de alto nivel para establecer los lineamientos en cuanto

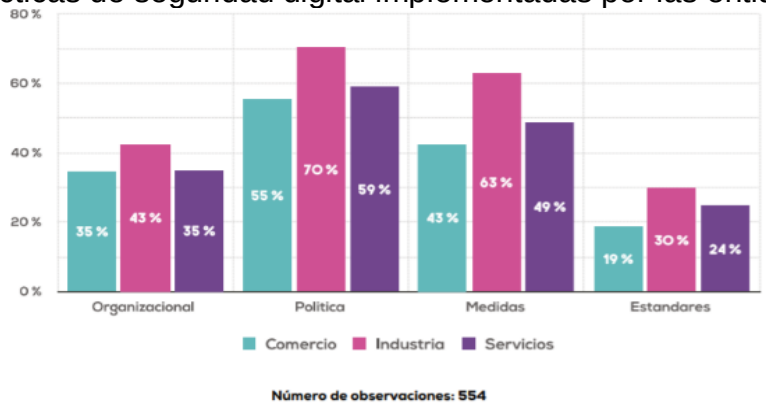
[42] BID, MINTIC, OEA. Estudio de Seguridad digital en Colombia. [En línea], 2017. [Citado el 2 de noviembre de 2018]. Disponible en Internet: <http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf>.

[43] Ibíd., p. 40.

acceso a sistemas, comunicaciones seguras, sensibilización, entre otros; por último, se encuentran las medidas técnicas cómo las pruebas de vulnerabilidades y el mantenimiento a la infraestructura tecnológica.

En la Figura 12 se aprecia que para "554 empresas encuestadas, se destaca el sector de la industria en cada una de las categorías, teniendo el 70% de prácticas de seguridad digital en políticas, seguido del 63% con el uso de medidas técnicas y el 30% con la implementación de estándares"[44]. Se observa que las políticas de la seguridad están enfocadas a que todos los usuarios deben conocer el alcance de esta declaración de alto nivel y especialmente aplicarla durante sus actividades cotidianas; seguido por las medidas técnicas que apoyan y complementan el acceso seguro a la información, sin embargo, se observa que un gran número de entidades no implementa ninguna practica de seguridad digital.

Figura 12. Prácticas de seguridad digital implementadas por las entidades



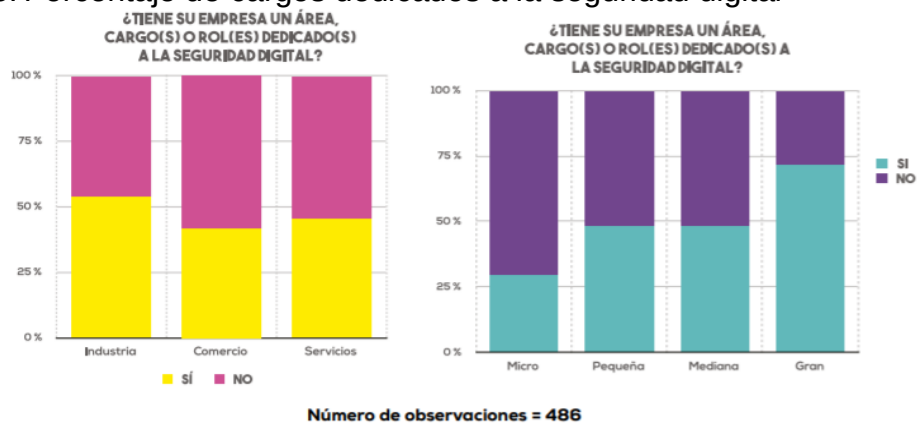
Fuente: BID, MINTIC, OEA. Estudio de Seguridad digital en Colombia. [En línea], 2017. [Citado el 2 de noviembre de 2018]. Disponible en Internet: <http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf>, pág. 41.

En la Figura 13 se tomaron en consideración "486 empresas encuestadas, dejando en evidencia un alto porcentaje de empresas medianas y pequeñas que no tienen una persona dedicada para la seguridad digital, este rol permite prevenir, detectar, identificar, resolver y mitigar posibles eventos de seguridad ante de que ocurran" [45]. Cuando este cargo es compartido con el área de tecnología, la seguridad pierde enfoque y eficiencia durante el proceso de aseguramiento de la infraestructura tecnológica de una organización.

[44] Ibíd., p. 41.

[45] Ibíd., p. 43.

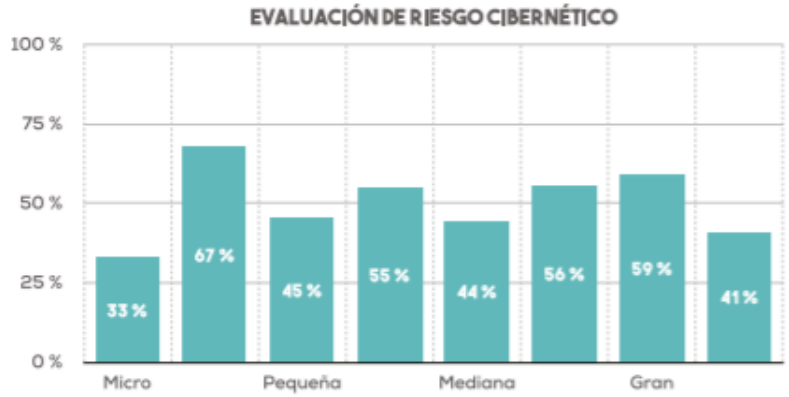
Figura 13. Porcentaje de cargos dedicados a la seguridad digital



Fuente: BID, MINTIC, OEA. Estudio de Seguridad digital en Colombia. [En línea], 2017. Disponible en Internet: <http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf>, pág. 43.

En cuanto a la evaluación de los riesgos tecnológicos, en la Figura 14 se presenta que la mayoría de empresas entrevistadas no realizan esta actividad. “La evaluación del riesgo le permite a una organización conocer el estado actual de la seguridad de la información, identifica riesgos potenciales que pueden impactar negativamente el negocio y propone una serie de salvaguardar para proteger los activos de la información”[46]. Por otro lado, las empresas que, si gestionan el riesgo, al parecer esta práctica no está alineada con estándares internacionales.

Figura 14. Evaluación del riesgo cibernético



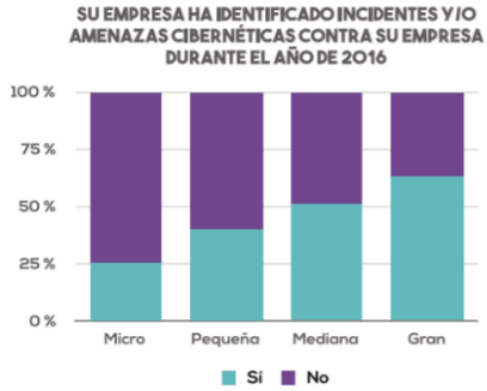
Fuente: BID, MINTIC, OEA. Estudio de Seguridad digital en Colombia. [En línea], 2017. Disponible en Internet: <http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf>, pág. 44.

[46] Ibíd., p. 44.

En la Figura 15 se observan que para “451 empresas entrevistadas, al referirse a temas de identificación de incidentes informáticos en contra de la empresa, el 63% de grandes empresas respondió afirmativamente, seguido del 51% de empresas medianas y 40% pequeñas empresas reconocieron haber presentado incidentes de seguridad digital”[47], con esto se demuestra que existe un gran número de empresas que no han presentado incidentes de índole informático o en su defecto no han identificado la presencia de ciberamenazas.

En el contexto colombiano, es preciso destacar que las organizaciones que han identificado incidentes y/o amenazas cibernéticas son aquellas que invierten recursos para la detección, predicción, análisis, mitigación y contención de incidentes digitales. Este hecho demuestra el nivel de madurez de las organizaciones y pone en evidencia que la ciberseguridad es una inversión a largo plazo que retorna su valor en la medida que evita sanciones, mantiene la operación segura de los procesos de negocio y protege la información.

Figura 15. Porcentaje de empresas que identificaron incidentes digitales



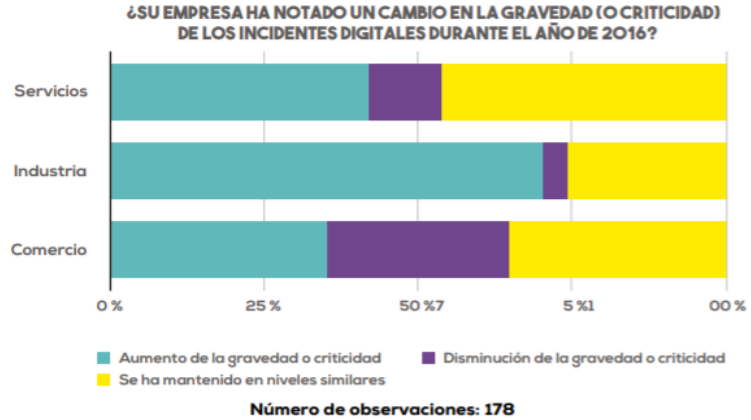
Fuente: BID, MINTIC, OEA. Estudio de Seguridad digital en Colombia. [En línea], 2017. Disponible en Internet: <http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf>, pág. 48.

En la Figura 16 se observa que “la mayoría de empresas entrevistadas del sector industria indicaron que la gravedad y criticidad de los incidentes informáticos aumento con respecto a eventos de seguridad ocurridos en años anteriores”[48], esto refleja que el avance de la tecnología conlleva a que las amenazas cibernéticas tengan un mayor impacto y generen consecuencias negativas en las operaciones tecnológicas de las organizaciones.

[47] Ibíd., p. 48.

[48] Ibíd., p. 52.

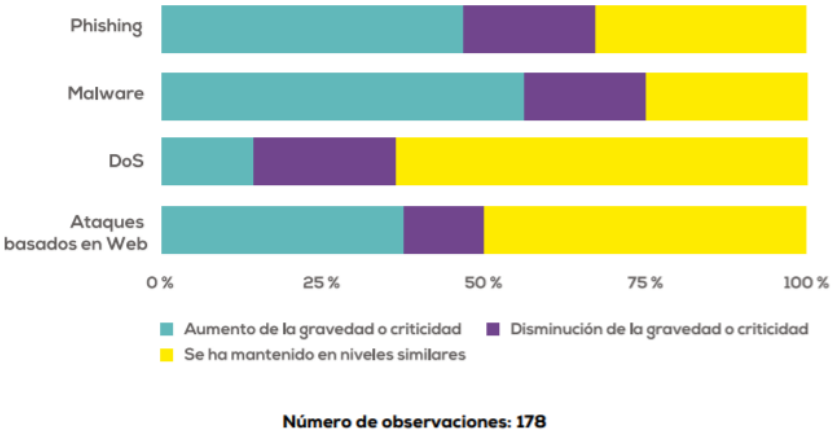
Figura 16. Cambio en la gravedad de incidentes digitales



Fuente: BID, MINTIC, OEA. Estudio de Seguridad digital en Colombia. [En línea], 2017. Disponible en Internet: <http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf>, pág. 51.

En la Figura 17 se aprecia el nivel de gravedad de incidentes para “178 empresas consultadas; los tipos de amenazas con mayor probabilidad de materialización son el *Malware, Phishing*, Ataques hacia páginas web y Denegación de Servicio”[49]. La tendencia marca claramente que los principales vectores de ataque esta orientados en el correo electrónico y las páginas web, 2 servicios críticos para cualquier empresa por su grado de adopción y usabilidad.

Figura 17. Gravedad de incidentes digitales



Fuente: BID, MINTIC, OEA. Estudio de Seguridad digital en Colombia. [En línea], 2017. Disponible en Internet: <http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf>, pág. 52.

[49] Ibíd., p. 54.

En la Figura 18 se aprecia que de un total de “250 empresas encuestadas, se asignó aproximadamente un presupuesto para la seguridad digital de 0.3% sobre de las ventas del año 2016”[50]. Esto deja en evidencia la falta de preocupación por la ciberseguridad en las organizaciones y cómo se desestima su verdadero valor en los procesos críticos y misionales.

Figura 18. Presupuesto anual para la seguridad digital

TAMAÑO DE LA EMPRESA	COP ($)	SECTOR ECONÓMICO	COP ($)
Micro	500 mil – 1 millón	**Comercio**	5 – 10 millones
Pequeña	5 – 10 millones	**Industria**	45 – 60 millones
Mediana	15 – 25 millones	**Servicios**	5 millones – 10 millones
Gran	120 – 140 millones		

Fuente: BID, MINTIC, OEA. Estudio de Seguridad digital en Colombia. [En línea], 2017. Disponible en Internet: http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf, pág. 60.

Tomando como referencia las entidades y organizaciones encuestadas que estimaron el costo de un incidente de seguridad informática, se establecieron 5 categorías en función de los costos ocasionados, para de este modo evaluar financieramente el impacto que puede generar la materialización de un incidente digital, las categorías son:

- Interrupción de las operaciones
- Daños a la infraestructura
- Sanciones, multas y gastos legales
- Daños a la reputación
- Perdida de la propiedad intelectual

Teniendo en cuenta la información presentada, se puede afirmar que las empresas colombianas en materia de seguridad digital tienen sus procesos definidos, sin embargo, para llegar al punto de la optimización de los procesos tecnológicos, hace falta mayor compromiso, presupuesto y conciencia por parte de la gerencia de las organizaciones que fueron objeto del estudio, lo cual es preocupante porque los ataques informáticos y sus correspondientes vectores cada día evolucionan y no esperan la maduración de la seguridad TI en las entidades ya sean de carácter público o privado.

[50] Ibíd., p. 60.

4.4 MARCO LEGAL

Durante el desarrollo del caso estudio se tienen en cuenta las normas implícitas en los escenarios planteados, además, se enfatizan las leyes nacionales relacionadas con el tratamiento y manejo de información sensible, uso y acceso a sistemas informáticos sin consentimiento previo, ejecución y distribución de software de manera ilegal, entre otros.

4.4.1 Ley 1273 de 2009 para Delitos Informáticos. "Es la normatividad que define los actos delictivos que utilizan las TIC (Tecnologías de la Información y la Comunicación), con el objetivo de comprometer la información y los datos de los colombianos y se establecen las penas y sanciones por tales conductas delictivas"[51]. Esta ley que aborda los castigos a todo aquel que se aproveche de la tecnología para sacar beneficio de los datos ajenos, por ende "la ley 1273 de 2009 establece categorías dependiendo la actividad delictiva asimismo las penas y sanciones pertinentes"[52]. En la Tabla 1 se mencionan los diferentes artículos que componen la ley de delitos informáticos en Colombia.

Tabla 1. Artículos de la ley de delitos informáticos 1273 de 2009

Articulo	Descripción
269 A	Acceso abusivo a un sistema informático
269 B	Obstaculización ilegitima de sistema informático red de telecomunicación
269 C	Interceptación de datos informáticos
269 D	Daño informático
269 E	Uso de software malicioso
269 F	Violación de datos personales
269 G	Suplantación de sitios web para capturar datos personales
269 H	Circunstancia de agravación punitiva
269 I	Hurto por medios informáticos y semejantes
269 J	Transferencia no consentida de activos

Fuente: COLOMBIA. MINTIC. Ley 1273 de 2009, De la protección de la información y de los datos. [En línea]. Disponible en Internet:<https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf>.

[51] COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Ley 1273 de 2009, De la protección de la información y de los datos. [En línea]. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf>.

[52] DACCACH, José. Ley de Delitos Informáticos en Colombia. [En línea]. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/>.

La ley de delitos informáticos en Colombia es un esfuerzo del gobierno colombiano para combatir las amenazas del ciberespacio y nace de la necesidad de proteger y salvaguardar los datos privados y la información confidencial de la sociedad colombiana. Para el escenario con enfoque técnico se identificaron los delitos cometidos y se contrastan con los artículos de la ley 1273 de 2009 para delitos informáticos en Colombia, la cual esta encarga de la tipificación y penalización de acciones hostiles por medios de herramientas tecnológicas.

4.4.1.1 Acceso no autorizado a una red de datos . Cuando un atacante accede de manera ilegal y no autorizada a una red, sin tener los permisos correspondientes, puede afectar la Confidencialidad, Integridad y Disponibilidad de la información privada y los activos de la información. Al tener acceso a la red se pueden realizar acciones de reconocimiento en busca de vulnerabilidades que le permitan obtener algún beneficio económico o de interés personal, además, en el peor de los casos se puede comprometer una máquina por medio de algún virus informático o realizar un ataque intencionado con el fin de modificar, eliminar, interceptar o generar información.

Se relaciona con este delito el artículo **269A. Acceso abusivo a un sistema informático**; un ciber delincuente que no estaba autorizado, tuvo acceso a la red de datos e información privada de los servidores, realizando la modificación no autorizada de la página web y sustracción de datos. Por este delito los delincuentes pueden tener una pena de 48 a 96 meses y pagar una multa de 100 a 1000 salarios mínimos. Otro artículo vinculado con esta conducta es el **269F. Violación de datos personales**, porque si una persona accede a una red de datos abusivamente, ya sea sin autorización o atacando los sistemas de seguridad, está violando el derecho a la privacidad de los datos personales.

4.4.1.2 Denegación de servicio. Este tipo de ataque afecta la disponibilidad de los recursos; cuando un atacante tiene acceso a la red de datos y establece conexión con un dispositivo o activo critico cómo por ejemplo un servidor, al no estar bien protegido el activo, es posible cambiar sus configuraciones, dejando fuera de servicio a los usuarios. Se vincula con este delito el artículo **269B. Obstaculización ilegitima de sistema informático o red de telecomunicación**; un ataque de denegación de servicio impide el normal comportamiento y operación de la red, generando sobre costos, indisponibilidad del servicio y revisiones por parte del personal especializado. Por este delito los delincuentes pueden someterse a una pena de 48 a 96 meses y cancelar una multa de 100 a 1000 salarios mínimos.

4.4.1.3 Monitoreo no autorizado de la red. Eeste tipo de acción afecta el pilar de la confidencialidad; se da cuando el atacante está escaneando la red en busca de paquetes IP que tengan la clave de acceso o información confidencial que se transmite en texto plano. Esta es la fase inicial de un ataque que busca acceder fraudulentamente a un sistema informático o red de datos. Se asemeja con este delito el artículo **269C. Interceptación de datos informáticos**; el simple hecho de ejercer monitoreo sin tener el previo permiso para hacerlo está catalogado cómo una conducta delictiva de captación de datos privados. Por este delito los delincuentes pueden tener una pena de 36 a 72 meses en prisión y no tiene multa económica.

4.4.1.4 Uso indebido de herramientas informáticas. Un atacante que use o desarrolle herramientas informáticas con fines maliciosos, está infringiendo el articulo **269E: Uso de software malicioso**, en el sentido que estas herramientas están creadas para generar un comportamiento no deseado sobre sistemas informáticos e irrumpen el flujo normal de los datos. Por este delito un delincuente puede tener una pena privativa de la libertad de 48 a 96 meses y costear una multa de 100 a 1000 salarios mínimos. Además, si el delincuente informático usa las herramientas digitales para sabotear o dañar algún activo tecnológico está infringiendo el articulo **269D. Daño informático**; el atacante logró tener acceso y sin estar autorizado alteró datos informáticos que no fue posible recuperar por falta de una copia de seguridad. Por este delito un delincuente puede tener una pena de 48 a 96 meses de cárcel y redimir una multa de 100 a 1000 salarios mínimos.

4.4.2 Ley 1581 de 2012 para la Protección de Datos Personales. "Es la normatividad que establece los lineamentos para el tratamiento de la información y la protección de los datos personales de los ciudadanos colombianos"[53]. Esta ley define los tipos de datos, responsables, mecanismos de vigilancia y control, así cómo procedimiento y sanciones en pro de proteger y resguardar los datos de los ciudadanos que han sido registrados en cualquier base de datos en el territorio nacional, además se protege de cualquier tipo de operación, recolección almacenamiento, uso, circulación o tratamiento por parte de organizaciones públicas y privadas. Su principal objetivo es garantizar privacidad de los datos y la intimidad a los colombianos, teniendo en cuenta la protección de los derechos fundamentales de la información personal, con base en el principio de confidencialidad para el buen uso de los datos personales e integridad para garantizar su estructura y sentido.

[53] COLOMBIA. SECRETARIA DEL SENADO. Ley estatutaria 1581 de 2012, protección de datos personales. [En línea]. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html>.

4.4.3 CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa. "En este documento se establece la política de seguridad cibernética para hacerle frente a las amenazas informáticas en el país, asumiendo una estrategia defensiva que le permite a los diferentes actores del estado actuar proactivamente ante un evento de seguridad informática" [54]. Se definen recomendaciones y controles para mitigar el impacto de un incidente de seguridad y se determinan las políticas de prevención y control para detectar posibles intentos de ataques informáticos y responder eficientemente ante una amenaza.

4.4.4 CONPES 3854 de 2016 Política Nacional de Seguridad Digital. Es un instrumento técnico que apoya las políticas nacionales y busca promover un entorno digital confiable y seguro, de tal manera que se identifiquen los riesgos que se generan al estar en línea y se maximicen los beneficios que generan el uso de las tecnologías de la información y las comunicaciones (TIC). "Con este documento se busca generar conciencia de tal modo que los ciudadanos puedan protegerse, prevenir y reaccionar proactivamente ante ciberataques"[55]. La política nacional de seguridad digital fundamenta su aplicación en la implementación de elementos educativos, penales incluyentes y abiertos para que cualquier ciudadano los pueda consultar.

4.4.5 Ley 1928 de 24 de julio de 2018 Convenio sobre la Ciberdelincuencia. Adoptado el 23 de noviembre de 2001, en Budapest, "este acuerdo internacional es un esfuerzo mancomunado por mantener un estrecho vínculo entre los estados y el sector privado para combatir el ciber crimen y las amenazas informáticas, asumiendo la cooperación en el marco legal, reforzando la normatividad y manteniendo una respuesta rápida y operativa"[56]. Dado que el cibercriminal utilizó herramientas tecnológicas para cometer la acción delictiva, sus actos están en contra de la presente ley, que busca combatir y erradicar la ciber delincuencia, preparando técnicas y controles tecnológicos en las organizaciones públicas y privadas.

---

[54] COLOMBIA. MINISTERIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Documento CONPES 3701, Lineamientos de política para ciberseguridad y ciberdefensa. [En Línea]. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf>.

[55] COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES 3854, Política nacional de seguridad digital. [En línea]. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>.

[56] COLOMBIA. PRESIDENCIA DE LA REPUBLICA. Ley 1928 24 de Julio de 2018. Convenio sobre la ciberdelincuencia. [En Línea], julio 2018. [Citado el 27 de noviembre de 2018]. Disponible en Internet: <http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf>

5. DISEÑO METODOLÓGICO

El caso estudio aplicado tiene como eje central la ciberseguridad en las organizaciones y se desarrolla basado en la observación y exploración aplicada desde una perspectiva práctica que se fundamenta en conocimientos teóricos, dicho en otras palabras, se pretende dar solución a un problema específico con aplicación práctica a partir de la teoría.

5.1 METODOLOGÍA DE INVESTIGACIÓN APLICADA

Se elige la metodología de investigación aplicada porque la motivación del presente proyecto es resolver un problema en un contexto particular para lo cual son necesarios el saber y el hacer, (conocimiento y práctica), así como también es pertinente sustentar el análisis de este proyecto bajo los siguientes criterios, según el Dr. Roberto Hernández[57].

- **Estudio explicativo y descriptivo**: Orientado a buscar el origen del ataque informático, y relacionar las causas con sus respectivos efectos para la empresa RANDOM S.A. Además, se mencionan los hechos tal y cómo son observados.

- **Método deductivo**: A partir del enunciado donde se detallan los hechos del ataque informático en la empresa RANDOM S.A, se pretende analizar el estado actual de la seguridad y generar las respectivas recomendaciones.

- **Análisis cualitativo**: El escenario está en tiempo presente y la situación inicial está apoyada en una descripción detallada, asimismo los datos suministrados son subjetivos y no se pueden manipular fácilmente. La información del evento de seguridad está basada en observación y descripción de lo sucedido durante el ataque.

- **Experimental**: Bajo un entorno de laboratorio controlando se quiere recrear el escenario para poder observar, analizar y determinar las causas que permitieron la materialización del ataque informático.

- **Bibliográfica y documental**: Es necesaria para contextualizar los diferentes conceptos encontrados en el enunciado de la situación problema, siendo fuentes primarias textos, monografías y textos académicos de ciberseguridad.

[57] Hernández, S., Fernández, C., y Baptista, L. Metodología de la Investigación (6ª Ed.). México: McGraw Hill Educación. ISBN: 978-1-4562-2396-0

5.2 TÉCNICAS APLICADAS

Para recolectar información relevante, pertinente y precisa relacionada con ataques informáticos se tomarán en cuenta diferentes fuentes de consulta tales cómo tesis de grado, libros, revistas, artículos digitales, páginas web, leyes, estándares y documentos reconocidas que están públicamente disponibles, la idea principal es fundamentar la investigación en hechos prácticos y datos estadísticos que permitan tener una concepción clara en cuanto a ciberseguridad vista desde un enfoque ofensivo.

Con base en el análisis previo del caso estudio, se busca simular fidedignamente los ataques informáticos expuestos, para lo cual se hará uso de herramientas informáticas, la virtualización de sistemas operativos y entornos de red, sin embargo, se debe tener claro que existen algún tipo de limitantes cómo por ejemplo, la infraestructura tecnológica de la entidad, puesto que no es posible conocer qué dispositivos integran la solución tecnológica, por ende las pruebas de *ethical hacking* se harán basándose en un entorno de red de área local, en ese sentido, los resultados pueden variar debido a que los ataques reales al parecer fueron ejecutados desde una red externa y el atacante tuvo que vulnerar diferentes medidas de seguridad.

- **Observación directa**: se tendrá contacto directo con el problema debido a que se simula el escenario planteado, por lo tanto, se recopila información de cada ataque informático basado en observar y detallar su comportamiento, para posteriormente registrar la información y analizarla.

- **Análisis documental**: estudio de documentación bibliográfica relacionada con ataques informáticos y ciberseguridad, que de cierta manera contrasta los resultados obtenidos con la observación directa. De este modo se pueden inferir similitudes, realizar analogías con incidentes similares y proponer posibles soluciones al problema.

- **Universo y muestra**: el escenario se origina en las sedes de Bogotá y Cali de la empresa RANDOM S.A, afectando directamente servidores que almacenaban la página web y las bases de datos. La población objetivo son los funcionarios del departamento TI que identificaron los ataques informáticos.

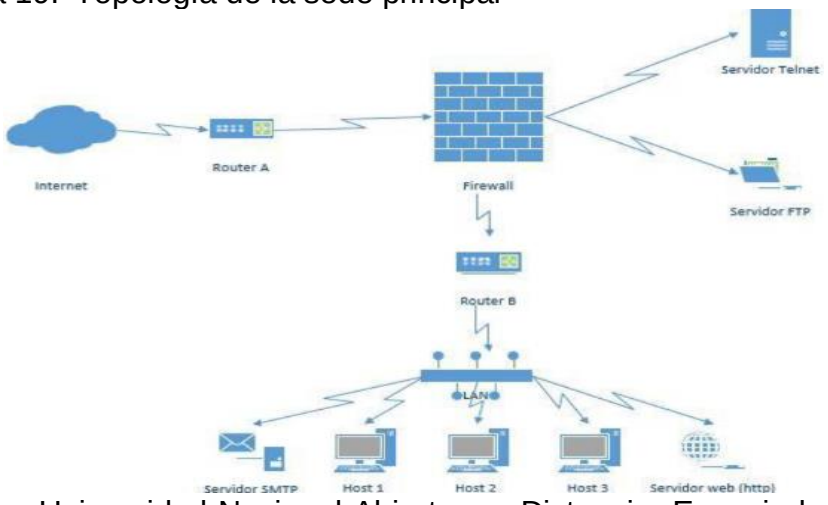
- **Normatividad**: para el desarrollo del caso estudio se emplean las metodologías OSSTMM y MAGERIT, enfocadas en las pruebas de penetración y análisis de riesgos respectivamente. Ambas metodologías son mundialmente reconocidas por los profesionales en ciberseguridad y se encuentran bien documentadas.

5.3 DESCRIPCIÓN DE LOS ESCENARIOS

A continuación, se describe el caso estudio compuesto de 2 enfoques, uno técnico y otro con administrativo, los cuales serán objeto de análisis durante el desarrollo del presente trabajo de grado.

5.3.1 Enfoque técnico. El pasado 01 de Julio de 2018 se presentó un ataque informático en la sede principal de la empresa RANDOM S.A ubicada geográficamente en la ciudad de Bogotá D.C., el ataque buscaba realizar un sabotaje y consistió en alterar la presentación de su portal web (Defacement), aprovechando una vulnerabilidad CGI (Common Gateway Interface) del lado del servidor. Este hecho generó que la disponibilidad, confidencialidad e integridad de la información almacenada en el portal web se vieran afectadas. Conforme al escenario planteado, se logró identificar que el servidor web Apache contaba con un módulo de phpMyAdmin el cual está instalado bajo un sistema operativo Linux Metasploitable 2.0, catalogado cómo sistema peligroso por ser vulnerable. Además, se pudo determinar que el ataque informático en la sede principal de la empresa RANDOM S.A fue ocasionado por un filtrado deficiente de paquetes en el dispositivo de seguridad perimetral y un esquema de seguridad bastante limitado; en la Figura 19 se observa la topología de la sede principal.

Figura 19. Topología de la sede principal



Fuente: Universidad Nacional Abierta y a Distancia. Enunciado del enfoque técnico, curso de proyecto de seguridad informática I. 2018. Disponible en Internet: < https://www.unad.edu.co/>

Después de la materialización del primer ataque, se presentó otro evento de seguridad en una sede de la empresa RANDOM S.A ubicada geográficamente en la ciudad de Cali. En esta ocasión, el servidor de esa sede fue comprometido por un ataque *EternalBlue* y los ciberdelincuentes extrajeron información sensible de repositorios y bases de datos propiedad de la organización, logrando así, comprometer la información privada y datos personales. Según el escenario planteado, se logró identificar que el equipo afectado tenía instalado un sistema operativo Windows 7 y el puerto 445 SMB (*Server Message Block*) estaba abierto y permitiendo conexiones. Tal puerto está asociado al ataque informático de ransomware "*Wannacry*". Además, el equipo atacado no contaba con la actualización MS17-010 la cual soluciona la vulnerabilidad de tipo SMB en sistemas operativos de Microsoft.

5.3.2 Enfoque administrativo. La empresa RANDOM S.A, pertenece al sector de tecnologías de la información, suministrando soluciones de red y telecomunicaciones a las empresas de Colombia, por medio de venta, configuración, administración e instalación de dispositivos de red y gestión de servicios telemáticos a precios asequibles. La organización cuenta con un recorrido en el sector de 16 años de experiencia y en la sede administrativa laboran 58 colaboradores entre directivos, administrativos y personal operativo, quienes garantizan la efectiva prestación del servicio a los clientes.

Debido al gran crecimiento organizacional durante el año 2019, la junta directiva ha tomado la decisión de incursionar con servicios para grandes compañías del país, por lo que la organización está reestructurando gran parte de sus áreas, entre ellas TI (Tecnología de la Información). Por esta razón, la junta le ha solicitado al director de TI la contratación de una persona que se haga responsable de la Ciberseguridad de la organización; esta persona se encuentra en proceso de selección e ingresará a la compañía el mes siguiente. RANDOM S.A. cuenta con algunos avances, sin embargo, no es preciso determinar el estado actual de sus políticas, procesos, estructuras e infraestructura tecnológica. De igual manera, no se reconoce un plan a corto y mediano plazo que determine el foco de las prioridades con respecto a los riesgos de seguridad informática y tampoco se cuenta con un marco de gobierno que permita garantizar que las iniciativas de seguridad están alineadas con los requerimientos de la organización.

6. RESULTADOS Y DISCUSIÓN

Este capítulo ha sido designado para mostrar el desenlace del presente proyecto aplicado, evidenciado el desarrollo de la metodología de gestión de riesgos MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), y el uso de la metodología OSSTMM (*Open Source Security Testing Methodology Manual*), para ejecutar las pruebas de penetración a los sistemas operativos de los servidores comprometidos.

6.1 IMPORTANCIA DE LA VIRTUALIZACIÓN

"La simulación es una técnica que se utiliza para reproducir procesos virtuales con el fin de analizar su comportamiento o aprovechar sus beneficios sin necesidad de tener el recurso físicamente; es utilizada para reproducir el comportamiento de manera lógica"[58]. Este modelo simplificado de la realidad es usado por dispositivos computacionales para recrear algún tipo de recurso, de tal forma que: "físicamente se cuenta con un dispositivo, pero lógicamente pueden ser 2 o más, claro está dependiendo de los recursos reales de la maquina anfitrión"[59].

La virtualización es una técnica utilizada para simular el funcionamiento y operación de un dispositivo o sistema informático, permitiendo recrear un componente físico de manera lógica, con lo que se logra obtener los beneficios de un equipo informático sin tener que mantenerlo físicamente. Actualmente, esta técnica tiene diferentes usos en el campo de la informática cómo, por ejemplo, la virtualización de servidores, entornos de aprendizaje y desarrollo, elementos de recuperación ante desastres, ambientes de prueba, entre otros. En el campo de la ciberseguridad, la virtualización toma un rol trascendental porque permite realizar pruebas de hacking ético sin afectar un equipo físico que se encuentra en producción, de tal modo que el profesional a cargo de realizar las pruebas de *pentesting* puede simular un entorno de trabajo de la vida cotidiana para analizar vulnerabilidades y fallos en la configuración con motivos profesionales o académicos. Además, la virtualización permite obtener una colección de herramientas profesionales de auditoria de sistemas en un solo equipo físico, reduciendo la complejidad y los costos cuando se realiza este tipo de evaluaciones.

---

[58] ESPAÑA. INSTITUTO TECNOLÓGICO DE ARAGÓN. Simulación de procesos. [En línea], [Citado el 13 de noviembre de 2018]. Disponible en Internet: <http://web.itainnova.es/elogistica/lineas-de-trabajo/logistica-inteligente/simulacion-de-procesos/>.

[59] DORDOIGNE, Jose. Redes informáticas, nociones fundamentales 5° Edición, Virtualización de aplicaciones. [En línea], [Citado el 13 de noviembre de 2018]. Disponible en Internet: <https://books.google.es/books?hl=es&lr=&id=Huwy1L0PEq8C&oi=fnd&pg=PA19&dq=virtualizaci%C3%B3n&ots=N__tdneRex&sig=758wZpTID1MUfVrNEk7iqkPcgOo#v=onepage&q=virtualizaci%C3%B3n&f=false>.

La virtualización es bastante importante porque es el mecanismo para la recreación de un escenario bajo un ambiente controlado donde el profesional puede investigar con mayor nivel de detalle un incidente digital, además, este modelo de trabajo exime al profesional de cualquier tipo de responsabilidad legal teniendo en cuenta que la evaluación de la seguridad no se estaría realizando directamente sobre el activo comprometido, también sirve como prueba para validar la eficacia y el comportamiento de un control tecnológico.

6.2 ENFOQUE TÉCNICO

El enfoque técnico inicia con el proceso de análisis de riesgos de los sistemas de información de la empresa RANDOM S.A; el objetivo de esta etapa es identificar los activos críticos, evaluarlos en función de las propiedades de la seguridad de la información y determinar el nivel de madurez de la organización. Este análisis sirve como punto de partida para abordar los incidentes informáticos y es una actividad obligatoria para cualquier SGSI (Sistema de Gestión de la Seguridad de la Información).

6.2.1 Evaluación y análisis de riesgos . Este proceso gira en torno a los activos dentro de un sistema informático y define métodos para calcular el riesgo asociado con base en la probabilidad y el impacto de una amenaza. Tales activos pueden estar expuestos a circunstancias adversas que los pueden degradar o afectar hasta el punto de deterióralos completamente, en ese sentido, cada activo posee unas características particulares que lo definen, y son estos atributos los que permiten clasificarlo para evaluar su importancia y dependencia de otros activos dentro de la organización.

6.2.1.1 Identificación de los activos de la información. El primer paso que propone la metodología MAGERIT es identificar plenamente todos los activos relevantes de la empresa con la finalidad de asegurar lo que realmente posee importancia para el negocio. Vale la pena resaltar que se toman las categorías de mayor relevancia para realizar la clasificación de activos, teniendo en cuenta únicamente las categorías que aplican al contexto de la organización. El reconocimiento de los activos de la información permite tener control sobre cómo están asignados los recursos de la organización, quien es el responsable del activo y como es utilizado. En el Cuadro 1 se encuentra registrado el inventario de activos de la empresa RANDOM S.A., según el tipo de activo y se asigna un identificador único con su correspondiente descripción.

Cuadro 1.Identificación de los activos en la empresa RANDOM S.A.

ID	TIPO DE ACTIVO	SUBTIPO DE ACTIVO	ACTIVO	DESCRIPCIÓN
RT01	Equipamiento Informático	Equipos de Hardware	Servidor FTP	Servidor donde se encuentra alojado el sistema para la transferencia de archivos.
RT02	Equipamiento Informático	Equipos de Hardware	Servidor HTTP	Servidor donde se encuentra alojado la página web de la empresa RANDOM S.A. y los aplicativos disponibles.
RT03	Equipamiento Informático	Equipos de Hardware	Servidor Telnet	Servidor donde se encuentra permitido el acceso remoto para validar y solucionar eventos operativos remotamente.
RT04	Equipamiento Informático	Equipos de Hardware	Servidor SMTP	Servidor donde se encuentra alojado y publicado el sistema para el intercambio de correo.
RT05	Equipamiento Informático	Equipos de Hardware	Servidor de Bases de Datos	Servidor donde se encuentra alojado el sistema motor de bases de datos, repositorio de información.
RT06	Equipamiento Informático	Equipos de Hardware	Computador Escritorio	Estación de trabajo que utilizan los funcionarios internamente para el desarrollo de sus actividades.
RT07	Equipamiento Informático	Redes y Comunicaciones	Router	Dispositivo activo de red que permite el direccionamiento de paquetes y la intercomunicación entre redes.
RT08	Equipamiento Informático	Redes y Comunicaciones	Switch	Dispositivo de interconexión utilizado con el fin de conectar equipos dentro de una misma red, ubicado en las sedes para adquirir escalabilidad.
RT09	Equipamiento Informático	Redes y Comunicaciones	Firewall	Dispositivo de seguridad perimetral que permite el filtrado de paquetes y la segmentación de la red corporativa.
RT10	Equipamiento Informático	Redes y Comunicaciones	IDS	Es un dispositivo que evalúa el comportamiento de la red y genera las respectivas alarmas basadas en reglas.
RT11	Equipamiento Informático	Redes y Comunicaciones	LAN	Conexión de área local la cual está compuesta por diversos elementos de red, con el objetivo de comunicarse entre sí los diferentes equipos y servidores.
RT12	Esencial	Servicio objetivo - plataforma	Portal principal de RANDOM S.A	Es la página web donde se publican noticias actuales de la entidad, aplicativos y medios para la interacción con los clientes.

Cuadro 1. (Continuación)

ID	TIPO DE ACTIVO	SUBTIPO DE ACTIVO	ACTIVO	DESCRIPCIÓN
RT13	Esencial	Servicio objetivo - plataforma	Dominio de Internet de la empresa RANDOM S.A	Es el nombre único que identifica al portal de RANDOM S.A. en Internet, el cual está asociado a una IP pública.
RT14	Información	Información Física y/o Digital	Base de datos de RANDOM S.A	Repositorio digital donde están los registros y datos de clientes.
RT15	Información	Información Física y/o Digital	Documentos ofimáticos	Información de uso interno almacenada en las estaciones de trabajo.
RT16	Información	Información Física y/o Digital	Archivo	Información física de uso interno almacenada físicamente en las sedes.
RT17	Instalaciones Físicas	Sede	Sede principal Bogotá	Es el edificio o recinto físico donde se ubica la sede principal de RANDOM S.A., ubicado en Bogotá.
RT18	Instalaciones Físicas	Sede	Sucursal regional Cali	Es el edificio o recinto físico donde se ubica la sucursal regional ubicada en Cali.
RT19	Personal	Usuario	Clientes	Usuarios que usan la página web de RANDOM S.A.
RT20	Personal	Usuario	Colaborador	Son los colaboradores de la empresa RANDOM S.A. que interactúan con el portal web.
RT21	Personal	Usuario	Departamento TI	Son los colaboradores encargados de mantener y operar el portal web y la infraestructura tecnológica.
RT22	Servicios	WWW	Consulta del portal principal	Servicio utilizado para realizar consultas relacionadas con los procesos misionales.
RT23	Servicios	Intercambio de archivos	Transferencia de archivos	Servicio utilizado para publicar documentación de interés público a los clientes.
RT24	Servicios	Mensajería	Correo electrónico	Servicio establecido como canal de comunicación entre funcionarios y usuarios.
RT25	Servicios	Comunicaciones	Acceso remoto	Servicio de acceso remoto para validar desde cualquier parte con internet.
RT26	Servicios	Comunicaciones	Internet	Servicio que permite la interconexión Internet.

Fuente: El autor, basado en la metodología MAGERIT, libro II – catalogo.

6.2.1.2 Valoración de los activos de la información. Asignar un valor ponderado a los activos de información permitirá establecer su importancia en la organización y así mismo clasificarlo jerárquicamente para evaluar su grado de relevancia. Esta valoración puede estar en términos numéricos (valoración cuantitativa) o determinada por niveles (valoración cualitativa). La valoración debe ser imparcial y objetiva, debido a que requiere la intervención de todos los interesados y colaboradores de la organización para obtener resultados más cercanos a la realidad y al contexto.

6.2.1.3 Dimensiones de la valoración . Son las características inherentes que tienen los activos de la información y permiten conocer el valor de su criticidad, dicho de otro modo, esta ponderación permite conocer el impacto de la degradación o la afectación sobre un activo en términos de Disponibilidad, Confidencialidad e Integridad, como propiedades esenciales. Siguiendo las recomendaciones hechas por MAGERIT, estas dimensiones se definen claramente para evitar malas interpretaciones. En la Figura 20 se encuentran las dimensiones de valoración acorde con estándares internacionales; estos criterios se tuvieron en cuenta para realizar la valoración de los activos.

Figura 20. Dimensiones de valoración

Sigla	Dimensión	Descripción
C	**Confidencialidad**	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].
I	**Integridad**	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].
D	**Disponibilidad**	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007].
A	**Autenticidad**	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008].
T	**Trazabilidad**	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].

Fuente: ESPAÑA. PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II - Catalogo. [En línea]. Disponible en Internet: <https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html>, pdf. pág. 15 – 17

Para evaluar cada activo con respecto a las dimensiones de valoración, se toma como referencia la escala propuesta por la metodología MAGERIT y se realiza la operación media aritmética que permite establecer de manera cualitativa o cuantitativa el valor del activo.

El resultado de esta evaluación es el listado de activos en función del impacto al negocio y los organiza por su nivel de criticidad para la organización. En la Figura 21 se observan los criterios de valoración definidos para medir la importancia de un activo.

Figura 21. Criticidad

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: ESPAÑA. PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro III - Técnicas. [En línea]. Disponible en Internet: <https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html >, pdf. pág. 6.

En la Cuadro 2, se detalla el listado de los activos identificados en la empresa RANDOM S.A., con su correspondiente evaluación cualitativa de las dimensiones de valoración, obteniendo el resultado ponderado que define la importancia del activo, acorde con la escala de criterios de criticidad.

Cuadro 2. Valoración de los activos en RANDOM S.A.

ID	ACTIVO	C	I	D	A	T	PONDERADO
RT01	Servidor FTP	9	10	10	7	8	Alto
RT02	Servidor HTTP	10	10	10	9	9	Muy alto
RT03	Servidor Telnet	8	9	10	8	8	Alto
RT04	Servidor SMTP	7	9	10	10	9	Muy alto
RT05	Servidor de Bases de Datos	10	10	10	9	9	Muy alto
RT06	Computador Escritorio	8	8	8	8	8	Alto
RT07	Router	8	9	10	8	7	Alto
RT08	Switch	8	9	10	8	7	Alto
RT09	Firewall	8	9	10	8	7	Alto
RT10	IDS	8	9	10	8	7	Alto
RT11	LAN	8	8	8	10	9	Alto
RT12	Portal principal	10	10	10	9	9	Muy alto
RT13	Dominio de Internet	8	8	9	7	7	Alto
RT14	Base de datos	10	10	10	9	9	Muy alto
RT15	Documentos ofimáticos	8	8	7	7	7	Alto

Cuadro 2. (Continuación)

ID	ACTIVO	C	I	D	A	T	PONDERADO
RT16	Archivo	7	7	8	5	8	Alto
RT17	Sede principal Bogotá	10	0	10	9	9	Alto
RT18	Sucursal regional Cali	7	0	8	5	7	Medio
RT19	Clientes	7	0	7	7	7	Medio
RT20	Colaborador de la organización	7	10	10	6	9	Alto
RT21	Departamento TI	10	10	10	9	9	Muy alto
RT22	Consulta de registros digitales	9	8	10	8	9	Alto
RT23	Transferencia de archivos	9	10	10	7	8	Alto
RT24	Correo electrónico	8	9	9	10	9	Muy alto
RT25	Acceso remoto	7	9	10	10	9	Muy alto
RT26	Internet	9	10	10	7	8	Alto

Fuente: El autor, basado en la metodología MAGERIT, libro II – catalogo.

La valoración de los activos permite evidenciar claramente que activos relevantes requieren aseguramiento basado en su clasificación y las dimensiones de la información, la probabilidad en función del impacto si se materializa una amenaza, nivel de tratamiento y la relevancia.

6.2.1.4 Caracterización de las amenazas. La siguiente fase de la metodología MAGERIT, consiste en reconocer e identificar las posibles amenazas a las cuales pueden estar expuestos los activos de información. Tales amenazas son eventos con una probabilidad de ocurrencia que pueden afectar a los activos, por lo tanto, es necesario determinar qué situaciones de peligro se pueden presentar y el tipo de impacto que se genera. Esta etapa es importante, porque dependiendo del tipo de amenaza es posible seleccionar los controles apropiados para mitigar un incidente de seguridad.

Las amenazas son consideradas como una situación o actor que representa un peligro para los activos de la información, lo cual está en función de la degradación, afectación o indisponibilidad del servicio que presta el activo. La valoración de las amenazas está en función del efecto que puede generar su materialización y la frecuencia con que se pueden presentar. Acorde con las recomendaciones establecidas por MAGERIT, respectivamente en las Tablas 2 y 3 se toman las escalas para determinar la degradación (magnitud), y probabilidad de ocurrencia, (frecuencia), de un evento adverso.

Tabla 2. Degradación del valor

Sigla	Descripción	Frecuencia	Complejidad
MA	Muy Alto	Casi seguro	Fácil
A	Alto	Muy alto	Medio
M	Medio	Posible	Difícil
B	Bajo	Poco posible	Muy Difícil
MB	Muy Bajo	Muy raro	En extremo difícil

Fuente: El autor, basado en la metodología MAGERIT, libro III – Técnicas.

Tabla 3. Probabilidad de ocurrencia

Sigla	Valor	Frecuencia	Probabilidad
MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: El autor, basado en la metodología MAGERIT, libro III – Técnicas.

La valoración del impacto mide qué tan perjudicial puede ser un evento si involucra un activo crítico para la organización y de qué manera afecta a los procesos críticos del negocio. Es decir, la estimación entre la probabilidad de materialización y el impacto ocasionado, también es conocido como el producto entre la frecuencia de ocurrencia de un riesgo y la magnitud que genera si se presenta. Este valor es contrastado con una escala definida, donde se estima la criticidad y urgencia que se le debe asignar al riesgo. En la Tabla 4 se encuentran las respectivas definiciones de los criterios que se tuvieron en cuenta para realizar la valoración del impacto de las amenazas.

Tabla 4. Valoración del impacto de las amenazas

Impacto	Criterio
Grave	La degradación del activo es fácil o casi segura y la valoración del activo puede ser muy o extremadamente alta que causa daños extremadamente o muy graves.
Alto	La degradación del activo es alta o muy alta y la valoración del activo puede ser alta que causa daños con cierta gravedad.
Medio	La degradación del activo es posible o difícil y la valoración del activo puede ser media que causa daños importantes.
Mínimo	La degradación del activo es baja o poco probable y la valoración del activo puede ser baja que causa daños menores.
Insignificante	La degradación del activo es muy baja y la valoración del activo es despreciable e irrelevante a efectos prácticos.

Fuente: El autor, basado en la metodología MAGERIT, libro III – Técnicas.

En la Cuadro 3, se registran las amenazas identificadas para el inventario de activos previamente realizado; con base en este listado de amenazas, se lleva a cabo la valoración de la probabilidad, la degradación y el impacto. Estas métricas relacionadas entre sí generan la ponderación del riesgo; con esto es posible clasificar los riesgos que deben ser abordados con prontitud y tener una idea clara del estado de la seguridad de la información, este es un paso fundamente que debe abarcar amenazas de diferente índole.

Cuadro 3. Identificación de amenazas en la empresa RANDOM S.A.

ID	Activo	Origen de amenaza	Descripción amenaza	Prob	Deg	Imp	Riesgo
SR1	Servidores	Ataques intencionados	Manipulación de los registros de actividad	Medio	Medio	Alto	Importante
SR2	Servidores	Ataques intencionados	Manipulación de la configuración	Muy alto	Muy Alto	Grave	Critico
SR3	Servidores	Ataques intencionados	Suplantación de la identidad del usuario	Alto	Medio	Alto	Importante
SR4	Servidores	Ataques intencionados	Abuso de privilegios de acceso	Muy alto	Muy Alto	Grave	Critico
SR5	Servidores	Ataques intencionados	Uso no previsto	Bajo	Medio	Bajo	Moderado
SR6	Servidores	Ataques intencionados	Alteración de secuencia	Muy alto	Muy Alto	Grave	Critico
SR7	Servidores	Ataques intencionados	Análisis de tráfico	Medio	Medio	Alto	Moderado
SR8	Servidores	Ataques intencionados	Modificación deliberada de la información	Muy alto	Muy Alto	Grave	Critico
SR9	Servidores	Ataques intencionados	Ataque destructivo	Medio	Medio	Medio	Moderado
SR10	Servidores	Ataques intencionados	Robo	Medio	Medio	Medio	Moderado
SR11	Servidores	Errores y fallos no intencionados	Errores de los usuarios	Medio	Medio	Medio	Moderado
SR12	Servidores	Errores y fallos no intencionados	Errores de configuración	Muy alto	Muy Alto	Grave	Critico
SR13	Servidores	Errores y fallos no intencionados	Errores de monitorización (log)	Medio	Medio	Alto	Importante
SR14	Servidores	Errores y fallos no intencionados	Deficiencias en la organización	Alto	Medio	Alto	Importante

Cuadro 3. (Continuación)

ID	Activo	Origen de amenaza	Descripción amenaza	Prob	Deg	Imp	Riesgo
SR15	Servidores	Errores y fallos no intencionados	Vulnerabilidad de los programas	Muy alto	Muy Alto	Grave	Critico
SR16	Servidores	Errores y fallos no intencionados	Alteración accidental de la información	Medio	Medio	Alto	Moderado
Fuente: El autor, basado en la metodología MAGERIT, libro II – catalogo.							

6.2.1.5 Estimación del riesgo. En esta fase se integran los niveles de tratamiento y las acciones que se deben tomar ante los riesgos identificados. Este es un proceso clave durante el análisis de riesgos, porque en esta etapa se proponen las medidas pertinentes ante los hallazgos. En la Figura 22, se muestra el mapa de calor donde están ubicados los riesgos con base en su criticidad.

Figura 22. Mapa de calor para la gestión del riesgo

MAPA DE CALOR							
PROBABILIDAD (P)	Muy Alto	5		SR5,SR7	SR1	SR6, SR8	SR2, SR4
	Alto	4		SR9	SR3	SR12	SR15
	Medio	3			SR10	SR13	SR14
	Bajo	2				SR11	SR16
	Muy Bajo	1					
NIVEL DE RIESGO			1	2	3	4	5
			Insignificante	Mínimo	Medio	Alto	Grave
			IMPACTO (I)				

Fuente: El autor, basado en la metodología MAGERIT, libro III – Técnicas.

El mapa de calor es una herramienta que ofrece una visual clara sobre cuáles son los riesgos que requieren ser tratados de manera urgente, dicho en otras palabras, permite priorizar los riesgos con base en su valoración; además permite controlar y administrar estratégicamente la gestión de riesgos. Cada riesgo es situado en una zona en particular; la zona de color rojo tiene mayor prioridad y los riesgos ubicados en esta zona deben ser tratados lo antes posible ya que son de carácter urgente y eventualmente pueden convertirse en un incidente. No obstante, los riesgos situados en otras zonas son importantes y también deber ser tratados; la diferencia radica en el tiempo y los recursos disponibles. En la Tabla 5 se mencionan las acciones principales que se sugieren para el tratamiento del riesgo.

Tabla 5. Medidas para el tratamiento del riesgo

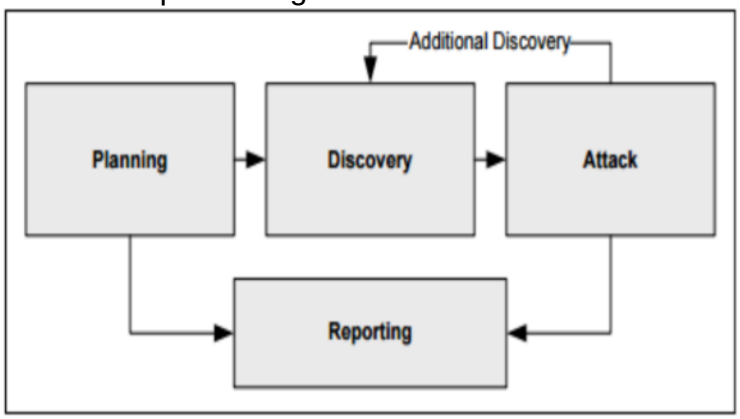
Acción	Descripción
Evitar	Acción tomada cuando el riesgo representa consecuencias negativas para la organización y es necesario plantear si el impacto que genera el riesgo puede evitarse al eliminar o suspender la actividad o proceso.
Prevenir	Establecer acciones anticipadas que lleven a que un evento no se materialice, entre las más comunes se encuentran la inspección, entrenamiento, mantenimientos, capacitaciones y sensibilización.
Proteger	Son aquellas medidas que se activan cuando el riesgo esta presenta, es decir se activa la salvaguarda o control de manera reactiva.
Aceptar	Asumir el riesgo y las consecuencias que trae consigo, ya que la evaluación no repercute en la operación o su impacto es positivo.
Retener	Proveer de planes y medidas que permitan volver a un estado normal, por ejemplo, los planes de contingencia o recuperación ante desastres.
Transferir	Asignar la responsabilidad del riesgo y su tratamiento a un tercero.
Diversificar	Es dividir el riesgo en diferentes áreas para que el impacto no sea tan alto como si el riesgo estuviera enfocado a un activo en particular.

Fuente: El autor, basado en la metodología MAGERIT, libro II – catalogo.

6.2.2 Pruebas de pentesting. La infraestructura, el personal y las aplicaciones tienen interacciones que deben ser analizadas y controladas para reducir los periodos de afectación y la perdida de la confidencialidad, integridad y disponibilidad. Una auditoria de seguridad informática ayuda a identificar brechas a nivel de configuración en los sistemas informáticos y detectar fallos de tipo operacional, administrativo o tecnológico. Para una organización consciente de la importancia de la ciberseguridad, las pruebas de hacking ético son una actividad necesaria que debe llevarse a cabo de manera rutinaria, lo cual le permite evaluar la efectividad de los controles y el nivel de preparación para afrontar un incidente de ciberseguridad. Para el caso de estudio se ha elegido la metodología OSSTMM, porque es un marco de trabajo completo que cuenta con bastante documentación en diferentes ámbitos en los cuales se realizan pruebas de seguridad. Esta metodología evalúa la seguridad en diferentes aspectos, (físicos, sociales y comunicaciones); esto se traduce en una comprensión profunda de los procesos de la organización y como se encuentran interconectados cada uno de sus componentes.

OSSTMM se destaca por su fase de análisis y la forma de responder los cuestionamientos de STAR (*Security Test Audit Report*). OSSTMM toma un concepto global de seguridad aplicado a pruebas de búsqueda de vulnerabilidades, auditorias, evaluación del riesgo, escaneos, y *hacking* ético. Transversalmente define el procedimiento y las actividades necesarias para comprobar los requerimientos de la seguridad; en la Figura 23 se observa el flujo e interacción de las fases de un *pentesting* basado en OSSTMM.

Figura 23. Fases de un pentesting basado en OSSTMM



Fuente: ESTADOS UNIDOS. National Institute of Standars and Technology. NIST 800-115 Technical guide to Information Security Testing and assessment. [En línea]. Disponible en Internet: < https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>, pág. 37

En el anexo A, se encuentra el listado consolidado de videos que registran cada una de las pruebas y técnicas ejecutadas en ambos escenarios del enfoque técnico.

6.2.2.1 Fase de planeación. Etapa preliminar donde se establece el alcance del *ethical hacking*, definiendo el acuerdo de confidencialidad sobre la información recolectada, además, se solicita la autorización formal del dueño o administrador del sistema para realizar las pruebas. Se definen las actividades a realizar y se identifican restricciones de tipo legal como normas y regulación vigente, y de tipo operativo; horarios y tiempos de ejecución de las pruebas.

6.2.2.2 Fase de descubrimiento. Etapa diseñada para recolectar información del sistema a auditar, está divida en las siguientes actividades:

- **Footprinting**: Tarea no intrusiva que busca obtener el mayor número de información del contexto, sistemas y componentes informáticos. Para esto se utilizan técnicas como ingeniería social, búsquedas avanzadas en internet, o identificar perfiles de usuarios en redes sociales.

- **Escaneo y numeración**: Tarea de identificación de sistemas disponibles, puertos a la escucha y servicios ofrecidos. Con base en la información recolectada se realizará un listado con todos los hallazgos. Es común en esta etapa utilizar herramientas como *Nmap* y *OpenVAS*.

- **Análisis de vulnerabilidades**: Tarea de pruebas y evaluación de vulnerabilidades basada en errores de configuración y brechas de seguridad en cuanto a ajustes o servicios expuestos. Por lo general se realiza una comparación entre el sistema a evaluar y los listados públicos de vulnerabilidades como el CVE, NVT o CWE, de tal modo que se comparen coincidencias y se descarten problemas de índole técnico.

6.2.2.3 Fase de ataque. Etapa central del hacking ético, que consiste en la materialización de la información recolectada, es decir que, con base en la información obtenida en etapas anteriores, se tiene pleno conocimiento de las debilidades con las que cuenta el sistema objetivo y se determinan los ataques que serán eficientes y con mayor porcentaje de éxito.

6.2.2.4 Fase de explotación. Tarea intrusiva que busca obtener acceso al sistema por medio de las vulnerabilidades identificadas, y en la que se utilizan *exploits* desarrollados en lenguajes de *scripting* como Python, Perl o Bash acorde con el objetivo a atacar. Es importante seleccionar adecuadamente el exploit a usar porque en ocasiones pueden comprometer el sistema hasta el punto de dejarlo fuera de servicio.

6.2.2.5 Fase de reporte. Etapa concluyente del hacking ético en la que se registran todos los hallazgos encontrados y se realiza la documentación formal, estableciendo un registro de cada uno de los pasos ejecutados en etapas anteriores. Adicionalmente, se realizan las recomendaciones a tener en cuenta para prevenir ataques y la sugerencia de controles tecnológicos que ayuden a resguardar el sistema de ataques reales.

En el anexo B, se detallan los procedimientos de respuesta ante incidentes de seguridad para cada uno de los ataques informáticos que componen los escenarios del enfoque técnico.

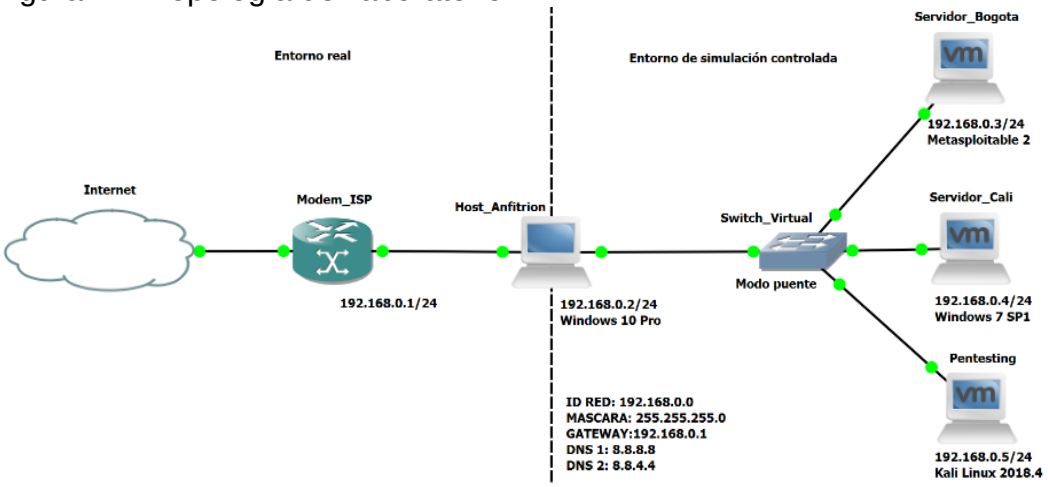
6.2.2.6 Descripción de la simulación. El escenario 1 consiste en virtualizar una maquina con sistema operativo Linux Metasploitable 2, para lo cual es necesario realizar la instalación completa de un programa de virtualización, que en este caso fue VirtualBox 5.2.22. La documentación recrea cada uno de los pasos durante el proceso de virtualización de los diferentes sistemas operativos.

Se debe tener presente que las máquinas virtuales utilizaran el adaptador de red en modo puente, lo que permitirá simular una red LAN con conexión a internet, tal como está configurado el Host anfitrión. Una vez se cuente con el sistema operativo Kali Linux instalado, es necesario actualizar los repositorios y paquetes. Después se procede a ejecutar las herramientas de *ethichal hacking* y se realiza el respectivo análisis de los resultados obtenidos. El escenario 2 consta de una maquina Windows 7

desactualizada y vulnerable a la cual se le realizará un ataque de tipo *Eternalblue* para obtener acceso a la ella y ejecutar algunos *payload* que permitan controlar periféricos.

En el anexo B, se encuentran los procedimientos de respuesta para cada uno de los ataques informáticos en cuestión. En la Figura 24 se presenta la topología sugerida para la elaboración del laboratorio controlado, es posible apreciar en esta imagen el direccionamiento y el rol que cada máquina desempeñará durante las pruebas del laboratorio controlado.

Figura 24. Topología del laboratorio



Fuente: El autor

- **Objetivo de la simulación.** Recrear los escenarios planteados para realizar los ataques informáticos de cada una de las sedes y, de este modo, identificar las vulnerabilidades en ambas maquinas servidor, analizar los puertos que se encuentran abiertos y ejecutar los ataques aprovechando los fallos de seguridad encontrados para, al final, realizar las recomendaciones pertinentes y aplicar los controles tecnológicos necesarios.

- **Alcance de la simulación.** La ejecución de cada uno de los ataques se realiza hacia 2 equipos tipo servidor, uno con sistema operativo Linux Metasploitable 2 y el otro cuenta con Microsoft Windows 7; el laboratorio controlado se plantea al interior de una red de área local (LAN). En ese sentido no se tienen en cuenta para realizar las pruebas de *ethical hacking* dispositivos de seguridad perimetral como firewall, sistemas de prevención de intrusos, (IDS), o equipos activos y *Routers*.

• **Recursos del laboratorio controlado.** En la Cuadro 4 están listados los elementos necesarios, de tipo software y hardware, para el desarrollo del laboratorio controlado.

Cuadro 4. Recursos necesarios para el laboratorio controlado

Elemento	Descripción	Función
(1) Equipo de escritorio	Procesador Core i7 7700 3.6 GHz, 16 GB de memoria RAM DDR4, 1 TB de Disco Duro, Windows 10.	• Elemento de hardware para realizar la virtualización y recopilar las evidencias.
Conexión a Internet	Ancho de banda de 3 Mbps, tipo ADSL.	• Necesaria para descargar el software necesario y realizar la actualización del S.O.
Ejecutable de Virtual Box	Versión 5.2.22, peso 108 MB,	• Software para virtualizar máquinas.
Imagen .iso Kali Linux	Versión Kali Linux 2018.3, peso 812 MB	• Disco de instalación del sistema operativo para ejecutar el *pentesting*.
Imagen .iso Tails	Versión Tails 3.11, peso 1,2 GB,	• Disco de instalación de la herramienta para el Deep web.
Imagen .zip Metasploitable	Archivo .vbox y vdi.	• Máquina virtual para realizar pruebas del servidor de la sede Bogotá.
Imagen .iso de Windows 7	Versión Profesional, SP1	• Disco de instalación del Sistema operativo del servidor de la sede Cali.
Fuente: El autor		

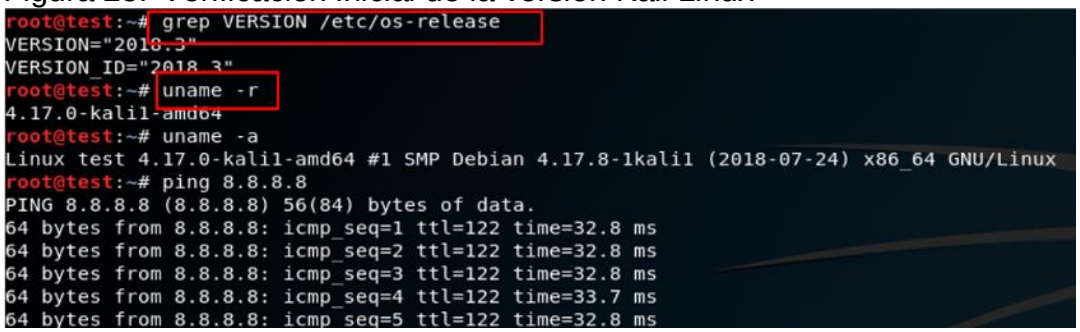
6.2.2.7 Simulación del ataque 1 – *Defacement.* A partir de este punto se muestra el desarrollo del escenario 1, donde se plantea simular un ataque de desfiguración a la página web principal de la empresa RANDOM S.A., el ataque es ejecutado por medio de la explotación de una vulnerabilidad sobre el componente CGI (*Common Gateway Interface*) del lado del servidor web Apache que ejecuta el lenguaje PHP. El vector de ataque utilizado es inyección de código, el cual consiste en enviar datos no esperados por el intérprete y de este modo acceder mediante una consola de línea de comandos al *kernel* del sistema operativo; después de tener acceso se edita a conveniencia del ataque la estructura del sitio web.

Usando la distribución Kali Linux, se ejecutan las diferentes herramientas de *pentesting* que permiten identificar y explotar vulnerabilidades del servidor objetivo. Este sistema operativo fue desarrollado por *Offensive Security*[60] y está diseñado específicamente para la auditoria de seguridad informática. Cuenta con un arsenal de más de 600 aplicaciones, está basado en Debian GNU/Linux y su predecesor fue BackTrack

[60] Offensive Security. [En línea]. 2018 Disponible en: < https://www.offensive-security.com/>

- **Actualización de Kali Linux.** Se cuenta con una máquina virtual de Kali Linux 2018.3 para evidenciar el proceso de actualización, además se prueba conectividad hacia Internet como requisito para la actualización. En la Figura 25 se observa la versión de la distribución Kali Linux mediante la ejecución del comando ***grep VERSION /etc/os-release***.

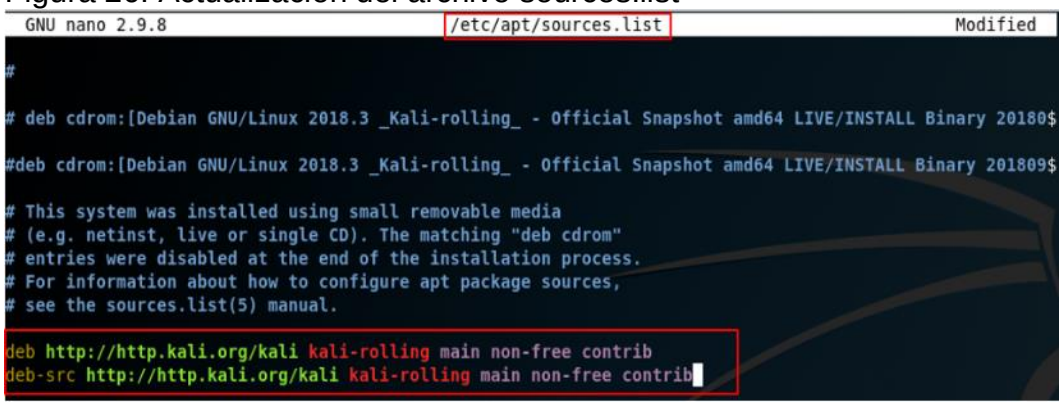
Figura 25. Verificación inicial de la versión Kali Linux



Fuente: El autor

Los repositorios permiten la descarga de paquetes binarios necesarios para la ejecución de las diferentes herramientas de Kali. Desde una terminal de comandos se digita el comando ***nano /etc/apt/sources.list*** para ingresar al archivo ***sources.list***. En la Figura 26 se aprecia la modificación del archivo de fuentes, donde se agregan los repositorios oficiales de Kali Linux.

Figura 26. Actualización del archivo sources.list

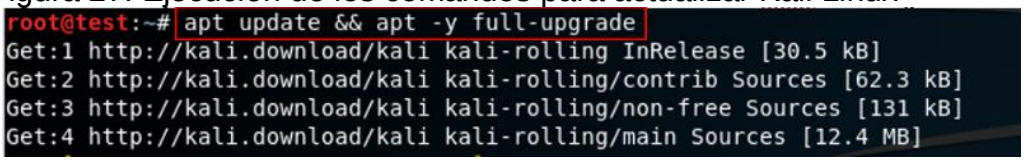


Fuente: El autor

El comando ***apt*** (*Advanced Package Tool*), sirve para la gestión de paquetes de software en distribuciones Linux, es decir permite descargar e instalar los diferentes componentes y aplicaciones del sistema operativo.

Con ***apt-update*** se actualiza el listado de paquetes disponibles en los repositorios y con ***apt-upgrade*** se instalan los paquetes previamente descargados según la configuración del sistema. Para realizar el proceso de actualización de Kali Linux, en la Figura 27 se muestra el comando ***apt update && apt -y full-upgrade***.

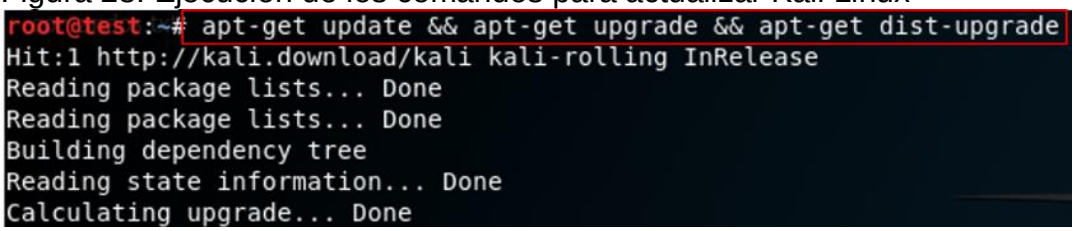
Figura 27. Ejecución de los comandos para actualizar Kali Linux



Fuente: El autor

En la Figura 28 se presenta otra manera de actualizar la distribución Kali Linux, mediante la línea de comando ***apt-get update && apt-get upgrade && apt-get dist-upgrade***. El comando ***apt-get*** es usado habitualmente por usuarios avanzados para tareas de bajo nivel y en la ejecución de scripts, por ende, para actualizar el sistema operativo Kali Linux se deben contar con privilegios de súper usuario *root*.

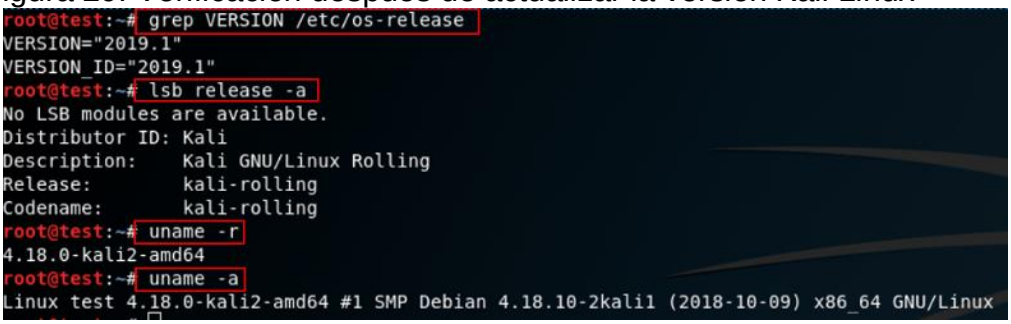
Figura 28. Ejecución de los comandos para actualizar Kali Linux



Fuente: El autor

Anualmente Offensive Security publica 4 actualizaciones al sistema operativo para ofrecer nuevas herramientas y corregir errores. El proceso de actualización de paquetes y versión de Kali Linux puede tardar un tiempo considerable dependiendo de los recursos físicos y ancho de banda de la conexión a Internet. Al finalizar este proceso se requiere de un reinicio de verificación para que el sistema se encuentre actualizado. En la Figura 29 se visualiza la ejecución del comando ***grep VERSION /etc/os-release*** para validar la versión del sistema después de la actualización, adicionalmente se incluye el comando ***uname –r*** para validar la versión del *kernel* y la arquitectura del sistema.

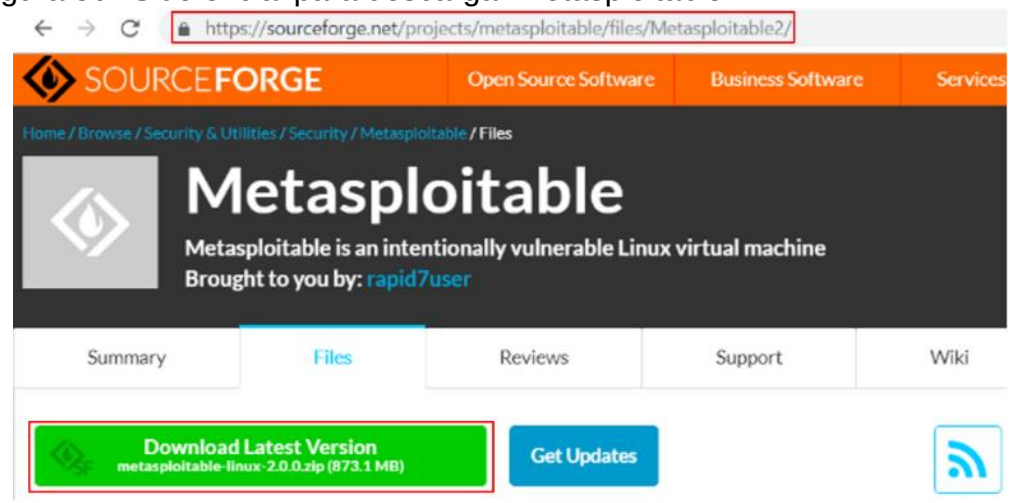
Figura 29. Verificación después de actualizar la versión Kali Linux



Fuente: El autor

• **Instalación de Metasploitable 2.0.** Desde el repositorio de *SourceForge*, se descarga el archivo comprimido en formato .zip que contiene la imagen de disco del sistema operativo Metasploitable 2. Al finalizar la descarga se debe guardar en una ubicación local de la máquina anfitrión y descomprimir el archivo para obtener la imagen pre-configurada. En la Figura 30 se muestra la página web oficial de descarga de la maquina Metasploitable-Linux, versión 2.0.0.

Figura 30. Sitio oficial para descargar Metasploitable 2

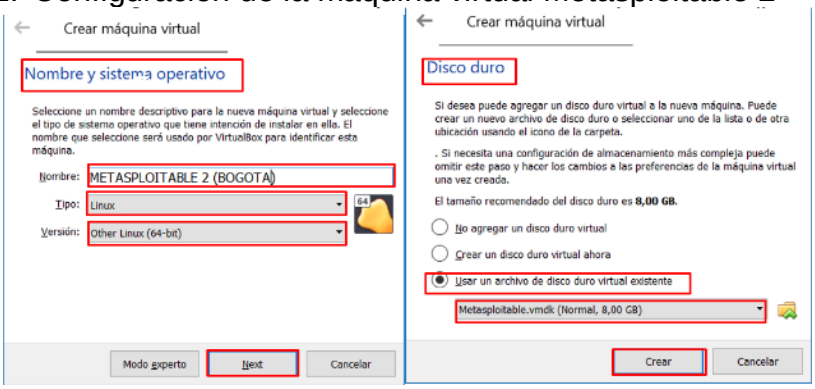


Fuente: El autor

En VirtualBox se procede a crear una máquina virtual, asignándole un nombre nemotécnico, recursos de memoria, CPU y red acordes con una maquina estándar de Linux; estas configuraciones no pueden sobrepasar las características de hardware del sistema anfitrión. Es importante tener en cuenta que el sistema debe tener compatibilidad para virtualizar bajo arquitecturas basadas en X64, es decir procesadores con instrucciones de

644 bits. En el ítem de ***Disco duro*** se elige la opción ***Usar un archivo de disco duro virtual existente*** para importar el archivo ***Metasploitable.vmdk***. Este archivo es un contendedor de disco duro virtual que tiene toda la configuración de la maquina Metasploitable 2. En la Figura 31 se expone la configuración de la máquina virtual del escenario 1.

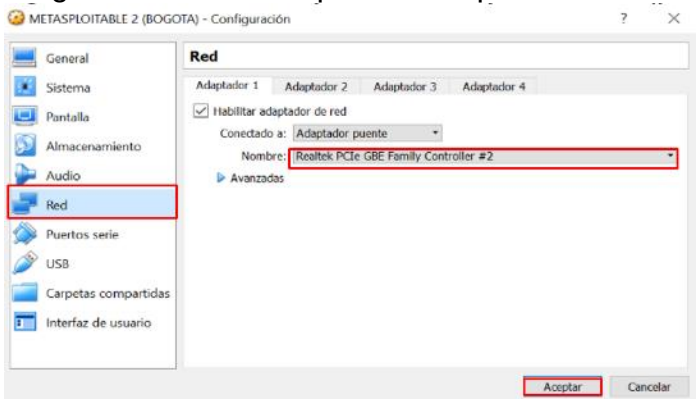
Figura 31. Configuración de la máquina virtual Metasploitable 2



Fuente: El autor

Al finalizar el asistente de configuración, se puede observar que la máquina virtual ha sido creada y está disponible en el menú lateral. Para modificar alguno de los ajustes establecidos se debe seleccionar la máquina virtual y elegir la opción ***configuración***, esto permite observar los ajustes de la máquina y modificarlos. Para el laboratorio, en la Figura 32 se indica que el adaptador de red queda en modo ***puente*** permitiendo establecer conexión entre máquinas virtuales, el host anfitrión e internet.

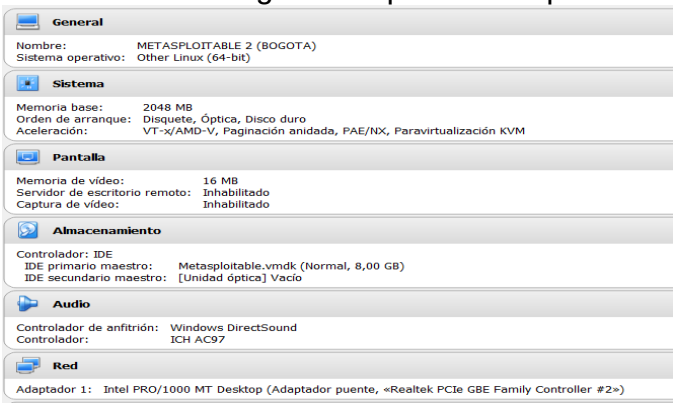
Figura 32. Configuración adicional para Metasploitable 2



Fuente: El autor

VirtualBox ofrece un resumen completo de las configuraciones de cada una de las máquinas virtuales creadas, esta opción se aprecia desde el panel lateral donde se presenta recuadro central. En la Figura 33 se visualiza la configuración completa de la máquina virtual Metasploitable 2.

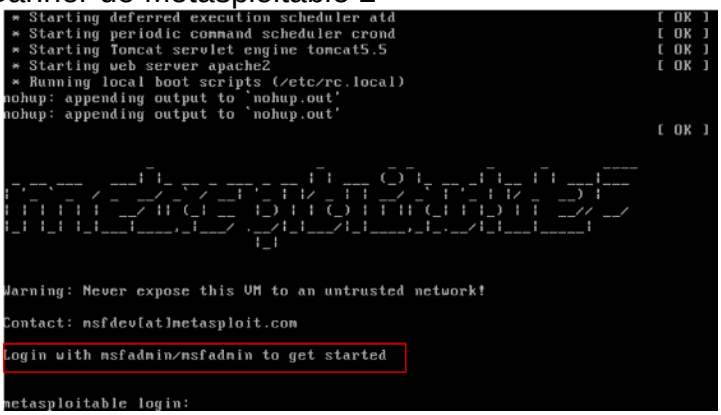
Figura 33. Resumen de la configuración para Metasploitable 2



Fuente: El autor

Con todas las configuraciones realizadas se selecciona la máquina virtual creada y se ejecuta la acción ***iniciar*** para dar marcha al sistema operativo; se observa la secuencia de inicio validando servicios y configuraciones preestablecidas. Vale la pena resaltar que esta máquina virtual ha sido desarrollada para ser vulnerable, mostrando en texto plano el usuario y contraseña para iniciar sesión, que para el caso práctico es ***msfadmin***. En la Figura 34 se aprecia el banner de acceso de Metasploitable.

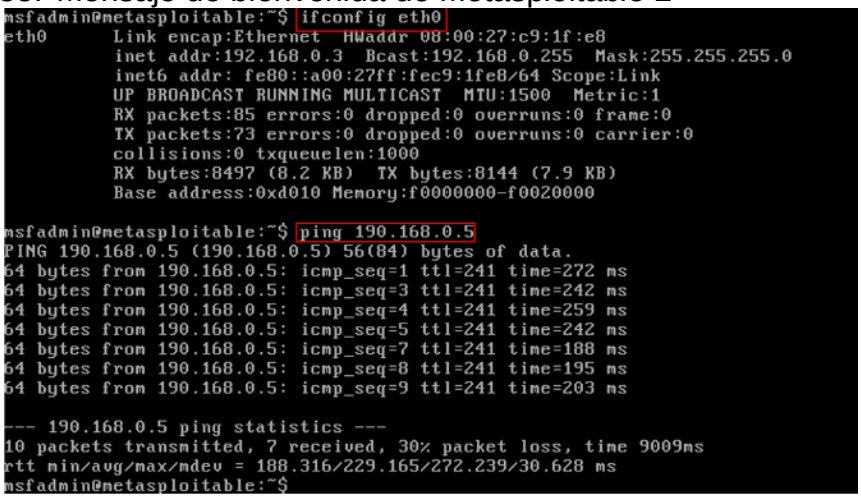
Figura 34. Banner de Metasploitable 2



Fuente: El autor

En la Figura 35 se observa el inicio de sesión y la configuración de red en la interfaz ***eth0***; después se valida conectividad hacia la maquina Kali Linux que será utilizada para ejecutar las pruebas de penetración y hacking ético.

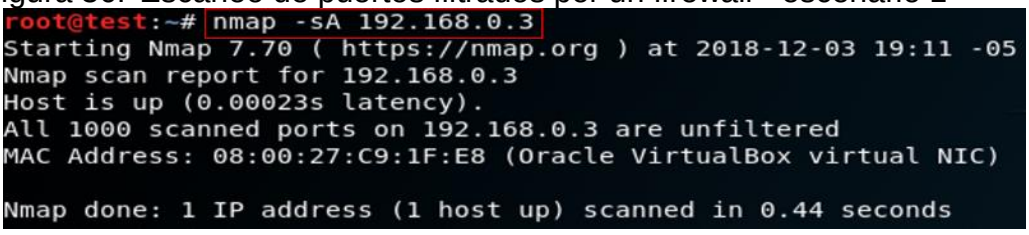
Figura 35. Mensaje de bienvenida de Metasploitable 2



Fuente: El autor

- **Escaneo de puertos con NMAP.** Nmap es un potente escáner para conocer los puertos que se encuentran en estado abierto y que servicios están activos en una máquina remota. En esta fase se pretende recolectar información relevante para llevar a cabo la explotación de vulnerabilidades e identificar si existe un firewall protegiendo la máquina. En la Figura 36 se aprecia la ejecución del comando *nmap –sA 192.168.0.3,* su salida muestra que ningún puerto está siendo filtrado, lo cual es un indicio que no existe ningún equipo perimetral que esté realizando el filtrado de paquetes.

Figura 36. Escaneo de puertos filtrados por un firewall - escenario 1

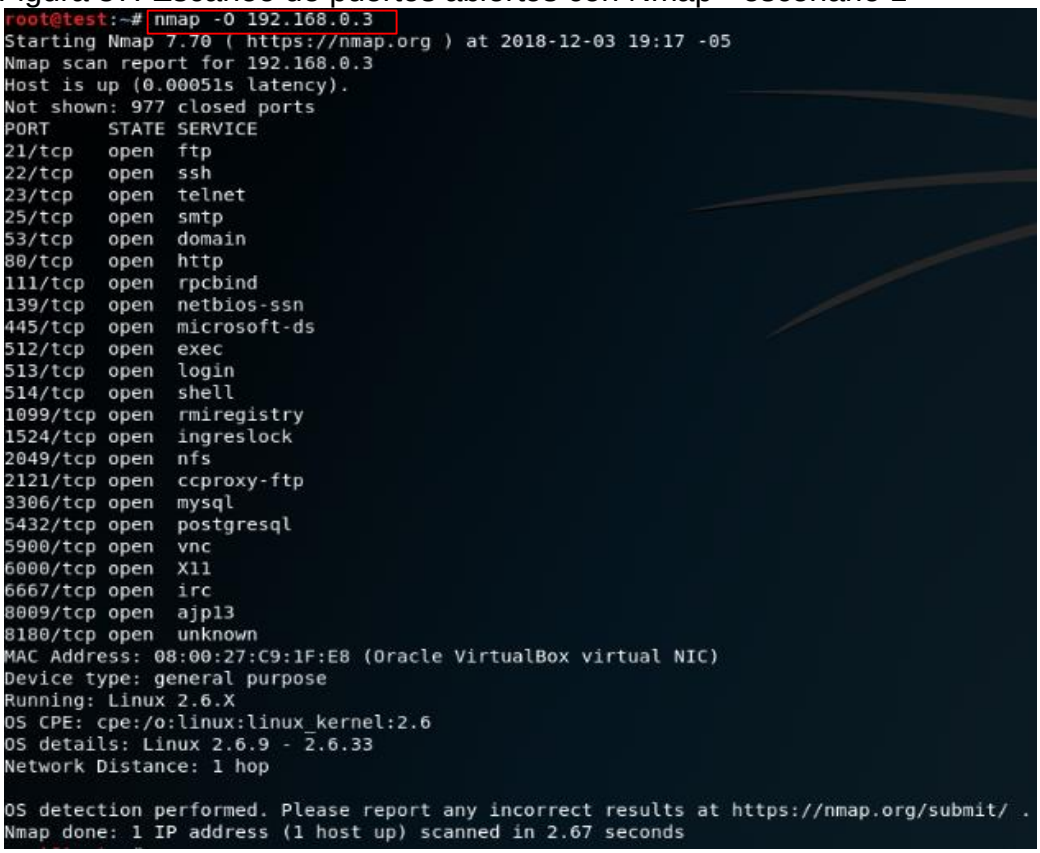


Fuente: El autor

El siguiente paso es ejecutar el comando ***nmap –O 192.168.0.3***, este comando permite tomar una huella del sistema operativo con base en el

tiempo de vida de un paquete. En la Figura 37 se observa la salida de este comando, identificando los puertos abiertos, la versión del *kernel* y que sistema operativo tiene la maquina a auditar.

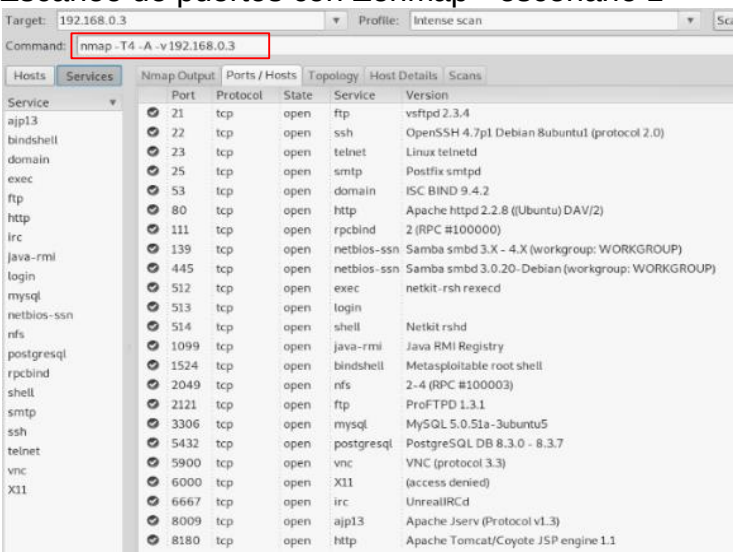
Figura 37. Escaneo de puertos abiertos con Nmap - escenario 1



Fuente: El autor

La etapa de enumeración es quizás la más importante en una auditoria de seguridad, debido a que su objetivo es recopilar la mayor cantidad de información referente al sistema a analizar, de tal modo que se tengan datos de usuarios, nombres de máquina, servicios de red, entre otros. Durante esta etapa se utilizan herramientas como Nmap y Zenmap; la sintaxis utilizada en ambas herramientas es la misma, la diferencia radica en que Zenmap cuenta con funcionalidades extra para recrear la topología, establecer perfiles de escaneo, enumeración de servicio y detalles de la maquina escaneada. En la Figura 38 se observa que la maquina a evaluar no está protegida por un firewall, además se identificaron 23 puertos abiertos y sus correspondientes servicios asociados.

Figura 38. Escaneo de puertos con Zenmap - escenario 1



Fuente: El autor

Conociendo los puertos y servicios abiertos de la maquina Metasploitable 2, es necesario identificar el software o aplicación que se está ejecutando con su correspondiente versión, para esto se digita el comando ***nmap –sV 192.168.0.3,*** en la Figura 39 se evidencian los resultados obtenidos.

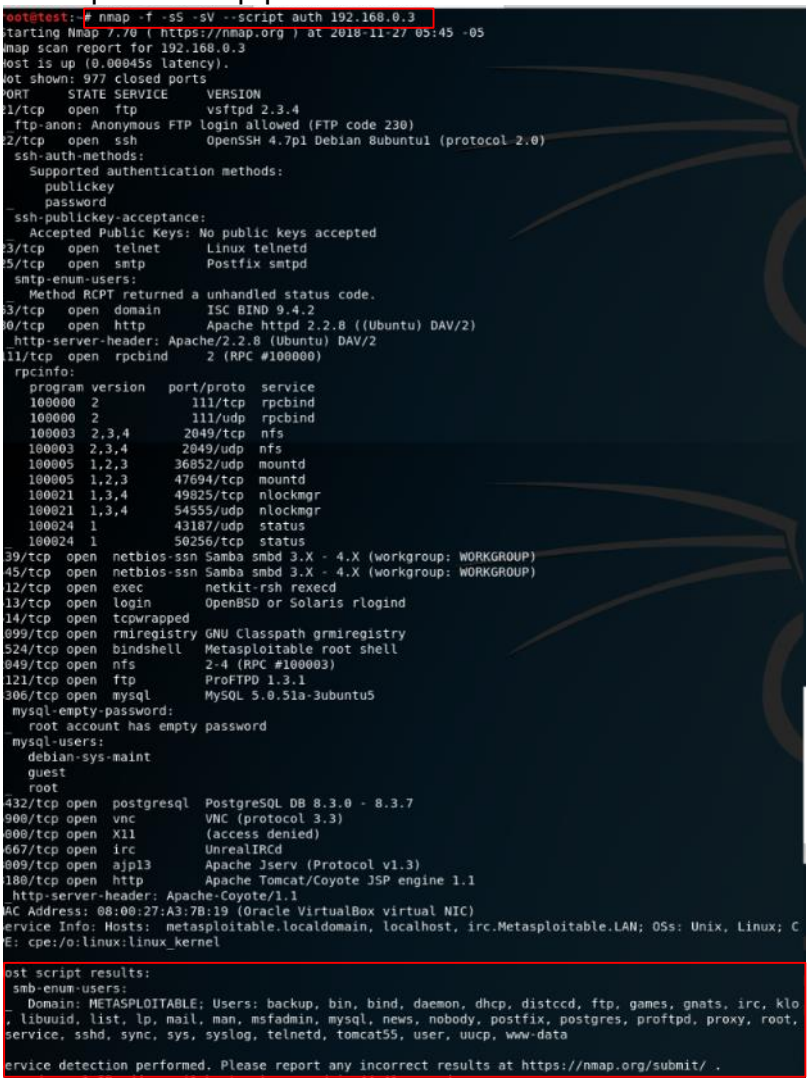
Figura 39. Verificación de aplicaciones y versiones - escenario 1

```
root@test:~# nmap -sV 192.168.0.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-03 19:18 -05
Nmap scan report for 192.168.0.3
Host is up (0.00022s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:C9:1F:E8 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; C
PE: cpe:/o:linux:linux_kernel
```

Fuente: El autor

Nmap cuenta con una función avanzada que permite realizar un escaneo profundo de manera automatizada por medio del uso de Scripts. Desde una terminal se digita el comando ***nmap -f -sS -sV --script auth 192.168.0.3***, que es un *script* automatizado para validar la autenticación en los servicios publicados. En la Figura 40 se aprecian las diferentes cuentas de usuario creadas en la maquina Metasploitable.

Figura 40. Script de Nmap para automatizar escaneo - escenario 1

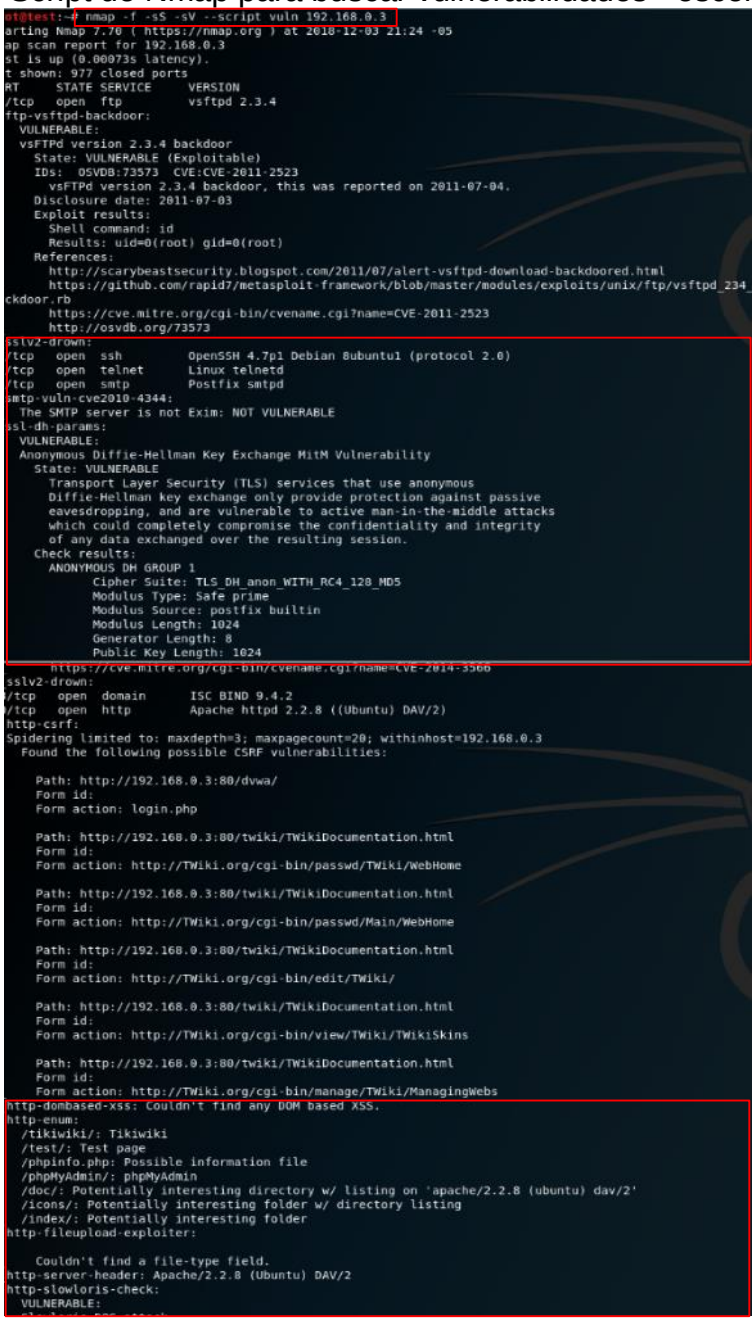


Fuente: El autor

Es interesante ver que Nmap tiene un motor de scripting, llamado NSE (*Nmap Scripting Engine*), que ofrece un script especializado para buscar y detectar vulnerabilidades conocidas. Para ejecutar este script se digita el

comando ***nmap -f -sS -sV --script vuln 192.168.0.3.*** En la Figura 41 se detalla el listado de vulnerabilidades identificadas en la maquina Metasploitable 2.

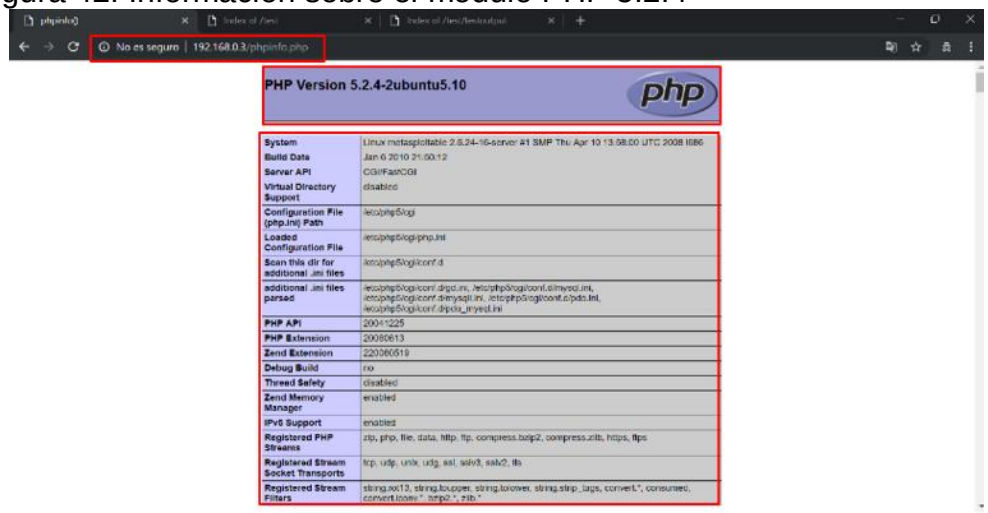
Figura 41. Script de Nmap para buscar vulnerabilidades - escenario 1



Fuente: El autor

Con el script de vulnerabilidades se identificó la URL (*Uniform Resource Locator*), que enlaza directamente con información de los diferentes módulos y documentación relacionada con el servidor web. En la Figura 42 se observa la información del módulo PHP, versión 5.2.4.

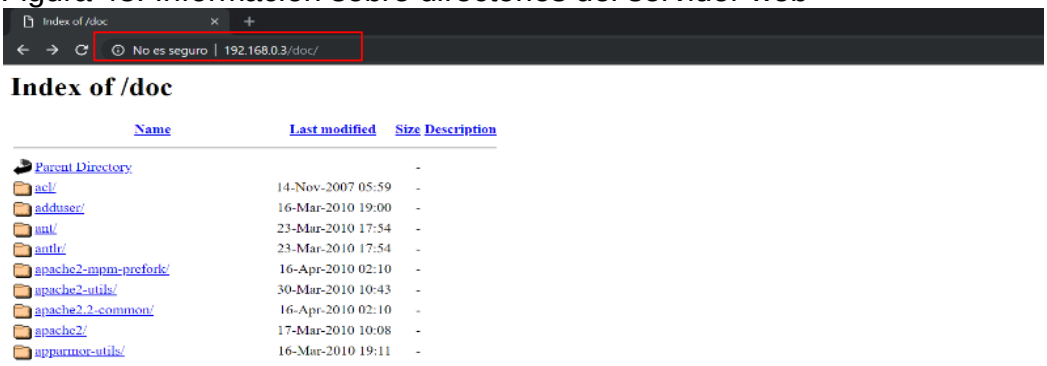
Figura 42. Información sobre el módulo PHP 5.2.4



Fuente: El autor

Otro hallazgo importante fue encontrar la ruta que permite la visualización de directorios y documentación de la configuración establecida en el servidor web. En la Figura 43 se observa el directorio */doc*, el cual contiene una serie de repositorios expuestos e información confidencial comprometida.

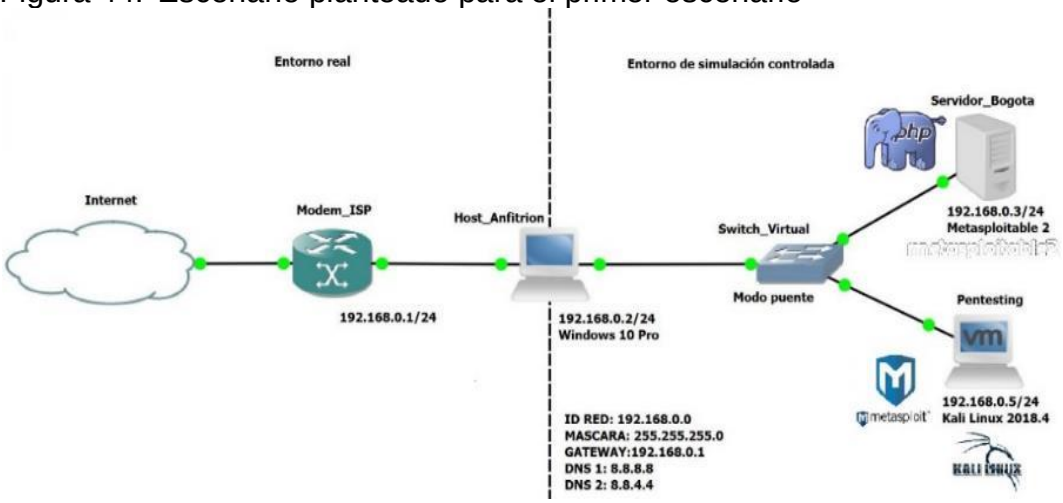
Figura 43. Información sobre directorios del servidor web



Fuente: El autor

• **Ataque CGI - PHP con Metasploit.** Con base en la información recolectada en la fase anterior, se ha identificado una vulnerabilidad que permite ejecutar código CGI (*Common Gateway Interface*) del lado del servidor web en su versión de Apache 2.2.8 y PHP 5.2.4; esta vulnerabilidad está relacionada con el código CVE-2012-1823: PHP CGI, según CVE[61]. En la Figura 44 se ilustra la topología para el desarrollo de este escenario, donde se cuenta con un ambiente de red de área local (LAN) por medio de la interconexión de un *switch* virtual, sin firewall de por medio.

Figura 44. Escenario planteado para el primer escenario



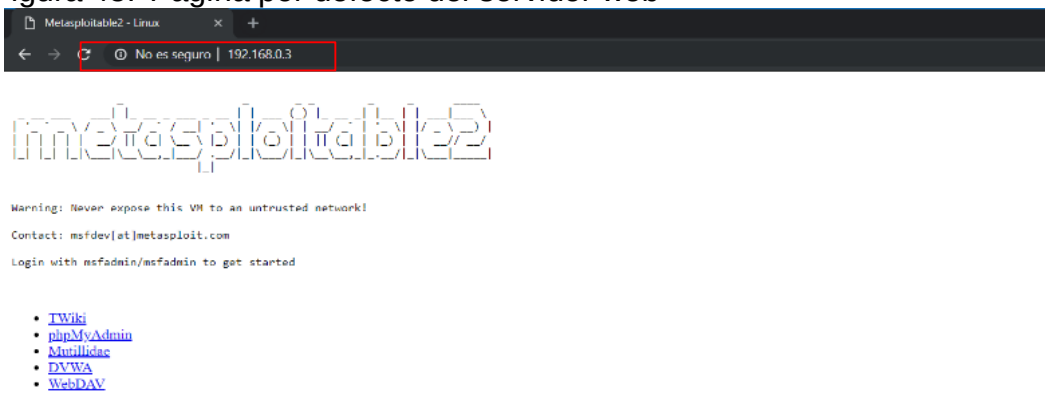
Fuente: El autor

Antes de iniciar la explotación de la vulnerabilidad sobre la página web que trae por defecto el servidor web de la maquina Metasploitable, es necesario utilizar un navegador web desde el host anfitrión para verificar que la página esté disponible. En la Figura 45 se puede apreciar que la página web presenta un conjunto de opciones y un mensaje de bienvenida similar al de inicio de sesión.

En la página web principal de Metasploitable 2 es posible interactuar con otro tipo de aplicaciones de entrenamiento como DVWA (*Damn Vulnerable Web Application*), *WebDAV, TWiki y Mutillidae*. Estos sitios web vulnerables han sido desarrollados para realizar pruebas de penetración bajo un entorno controlado; exponiendo las principales vulnerabilidades sobre aplicaciones web según el marco de referencia OWASP.

[61] Common Vulnerabilities and Exposures, CVE-ID CVE-2012-1823. [En línea]. 2018 Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823

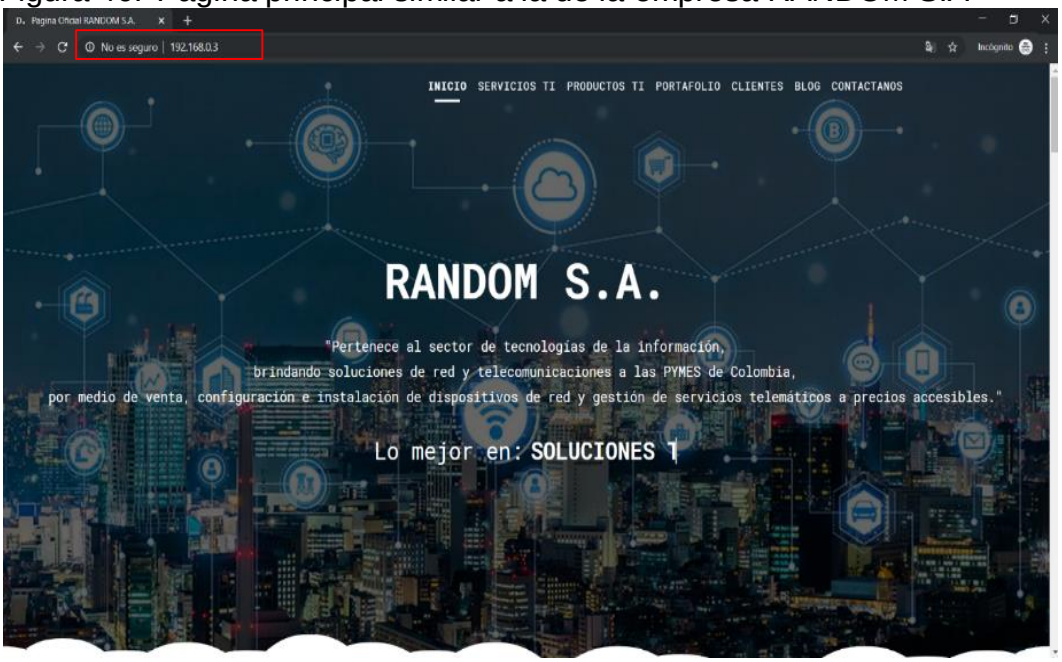
Figura 45. Página por defecto del servidor web



Fuente: El autor

La máquina Metasploitable trae por defecto una página web principal con un diseño bastante limitado, por lo tanto, se procede a realizar una copia del código HTML (*HyperText Markup Language*) del portal principal y se carga en el servidor web una réplica, pero con extensión PHP (*Personal Hypertext Processor)*. En la Figura 46 se observa la página web réplica de la empresa RAMDOM S.A.

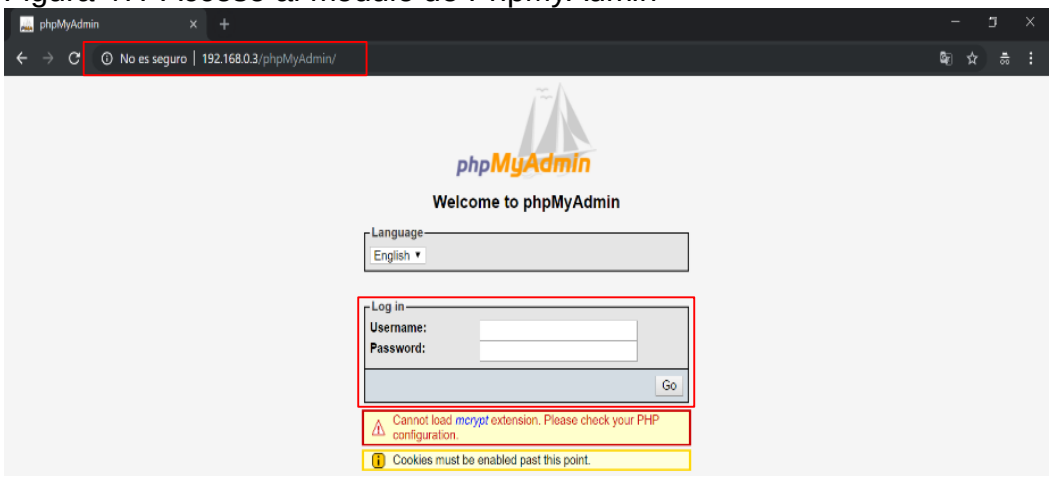
Figura 46. Página principal similar a la de la empresa RANDOM S.A



Fuente: El autor

En la Figura 47 se visualiza la página de acceso al módulo web de phpMyAdmin, el cual está divulgado sin ningún control y permite la gestión de las bases de datos almacenadas en el servidor del escenario 1.

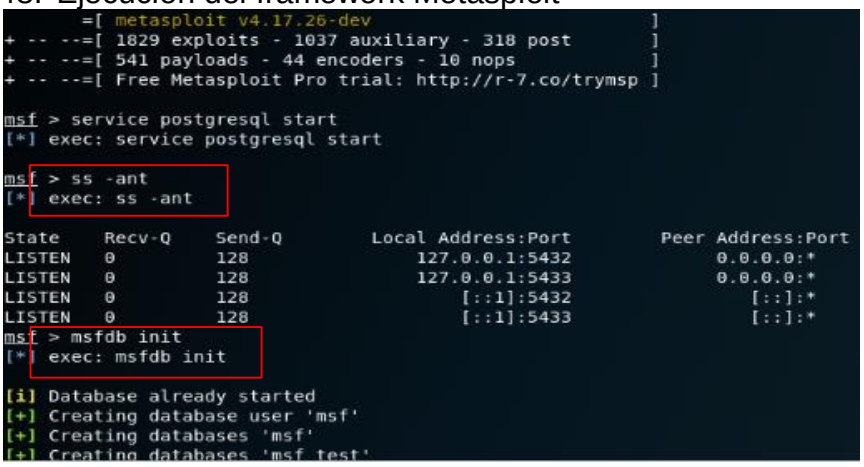
Figura 47. Acceso al módulo de PhpMyAdmin



Fuente: El autor

En la Figura 48 se observa el inicio del ataque cuando se ejecuta la herramienta Metasploit, "***msfconsole***", como súper-usuario, ***root***; después se inicializan los servicios requeridos por medio de los comandos *postgresql* (***service postgresql start***), puertos (***ss -ant***) y base de datos del *framework* (***msfdb init***).

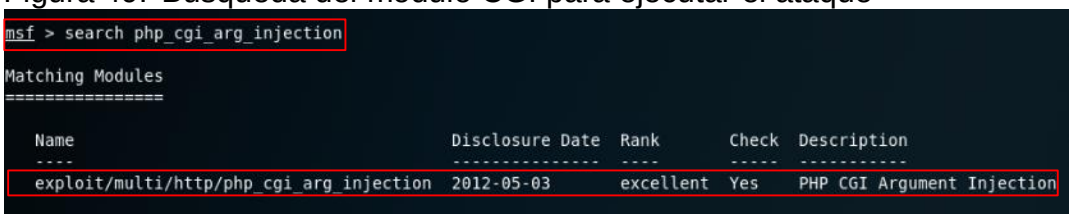
Figura 48. Ejecución del framework Metasploit



Fuente: El autor

Es necesario verificar si existen *exploit* para ejecutar el ataque de tipo CGI, por lo tanto, se ejecuta el comando ***search*** acompañado de un parámetro para realizar la búsqueda, en este caso, en la Figura 49 se especificó ***php_cgi_arg_injection*** para que la consulta fuera más eficiente.

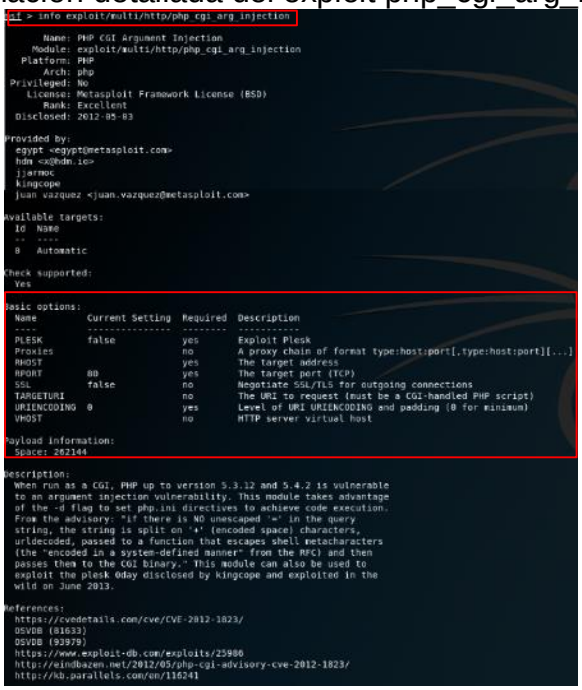
Figura 49. Búsqueda del módulo CGI para ejecutar el ataque



Fuente: El autor

Una vez identificado el exploit que será utilizado, se debe buscar información detallada del exploit a través del comando ***info exploit/multi/http/php_cgi_arg_injection***. La información detallada del *exploit* se observa en la Figura 50.

Figura 50. Información detallada del exploit php_cgi_arg_injection

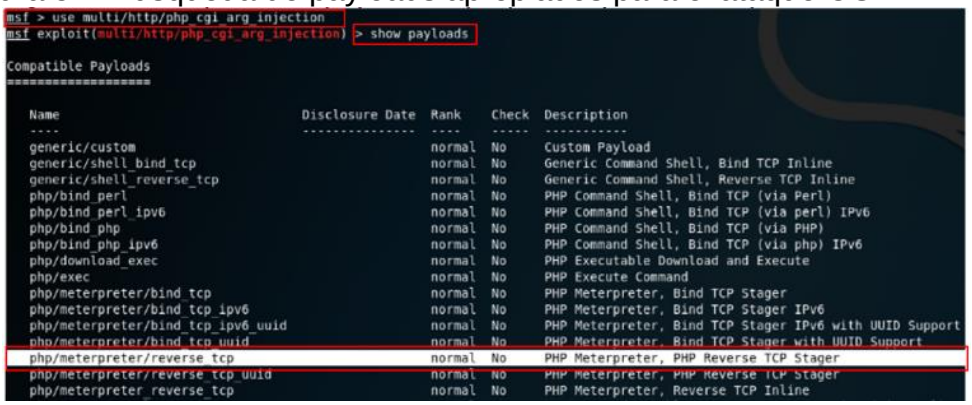


Fuente: El autor

El exploit ***exploit/multi/http/php_cgi_arg_injection*** fue publicado el 03/05/2012 y se utiliza en versiones de PHP inferiores a 5.3.12 y 5.4.2 que son vulnerables a la inyección de argumentos en el *flag –d* estableciendo ejecución de código en las directivas de php.ini.

En la Figura 51 se digita el comando ***use multi/http/php_cgi_arg_injection*** para seleccionar el *exploit* y su complemento, que para el caso se trata de un *payload* que permite ejecutar funciones específicas y comprometer la maquina víctima, generando un comportamiento no deseado como lo es el *Defacement* de la página web principal. Por medio de la opción ***show payloads*** se observa el conjunto de *payloads* disponibles para el *exploit* de inyección de código CGI, además, se observa que el *payload* que se ajusta al ataque es ***php/meterpreter/reverse_tcp***.

Figura 51. Búsqueda de payloads apropiados para el ataque CGI

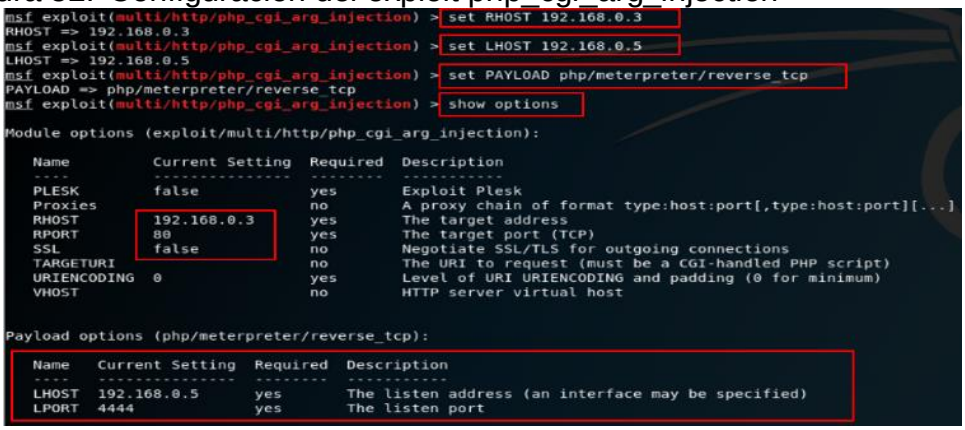


Fuente: El autor

Hasta este punto del laboratorio se cuenta con los datos necesarios para ejecutar el ataque informático, por lo tanto, se configura la herramienta Metasploit con la información del host remoto vulnerable (***RHOST***), el host local que va a ejecutar el exploit (***LHOST***), la carga útil, mejor conocido como el *payload* seleccionado (***php/meterpreter/reverse_tcp***), por último se muestra las opciones de configuración con el comando ***show options.***

Varias herramientas de monitoreo relacionan el puerto 4444 con software malicioso y *framework* de *Ethicak Hacking*, sin embargo, un atacante puede modificar este parámetro para evitar la detección de un SIEM (*System Information Event Management*). En la Figura 52 se observa la configuración del exploit ***php_cgi_arg_injection***.

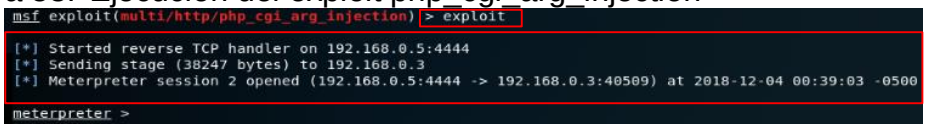
Figura 52. Configuración del exploit php_cgi_arg_injection



Fuente: El autor

En la Figura 53 se observa la ejecución del comando ***exploit,*** inmediatamente se inicia la conexión inversa TCP y si todo sale bien, se establece la sesión con el intérprete de comandos ***Meterpreter.***

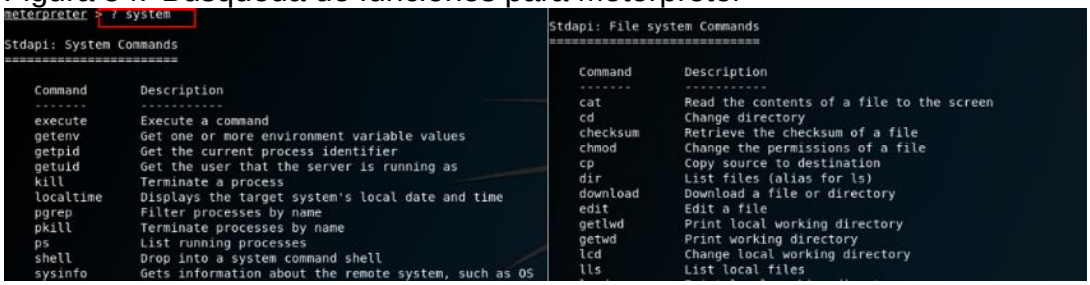
Figura 53. Ejecución del exploit php_cgi_arg_injection



Fuente: El autor

Meterpreter ofrece diferentes funciones y herramientas para comprometer la maquina víctima. En la Figura 54 se aprecia el listado de comandos disponibles; para obtener esta ayuda se debe preguntar con el signo **"?"**, solo o acompañado de una palabra clave.

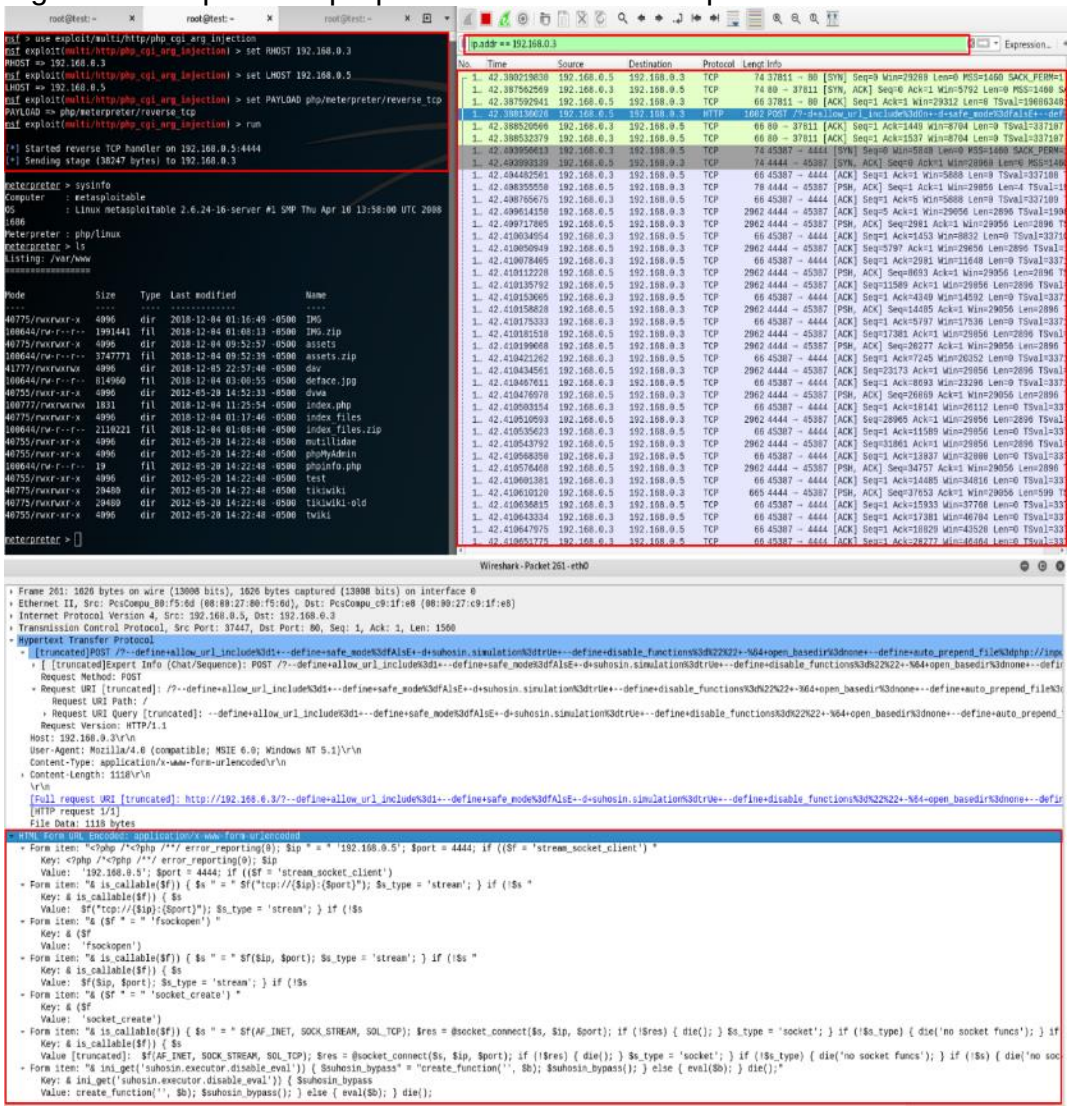
Figura 54. Búsqueda de funciones para Meterpreter



Fuente: El autor

Durante la ejecución del ataque se realizan capturas de paquetes por medio del analizador de protocolos Wireshark; se observa claramente la interacción y flujo de conexiones desde la maquina atacante hacia la maquina vulnerable. En la Figura 55 se logra identificar que el ataque inicia con una petición al puerto 80 donde se realiza la inyección del código CGI y se configuran los parámetros para realizar la conexión reversa TCP; después se inicia la ejecución del *Payload* y se establece una sesión de *Meterpreter* remotamente.

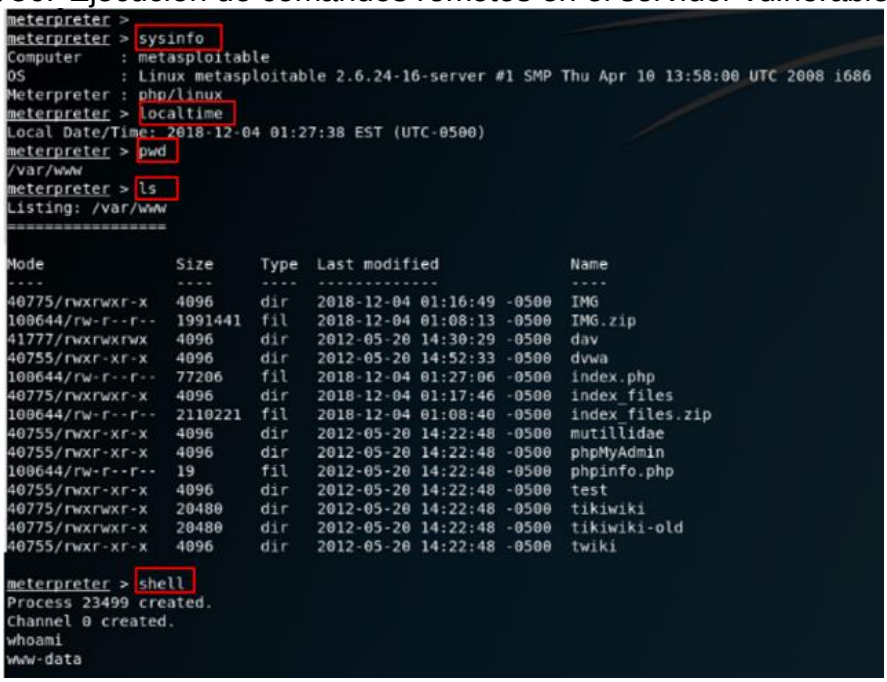
Figura 55. Captura de paquetes al realizar el ataque CGI



Fuente: El autor

Tras comprometer la máquina servidor, se usan comandos de meterpreter como ***sysinfo*** para conocer información del sistema, ***localtime*** para saber la configuración de fecha y hora, ***pwd*** para saber en qué directorio está situado y ***ls*** para listar el contenido del directorio actual. En la Figura 56 se evidencia control sobre la máquina ***metasploitable*** con los permisos del usuario ***www-data*** en el directorio ***/var/www***. Este hallazgo es de suma importancia porque deja al descubierto la ruta donde están almacenados los sitios web del servidor y sus correspondientes archivos de configuración.

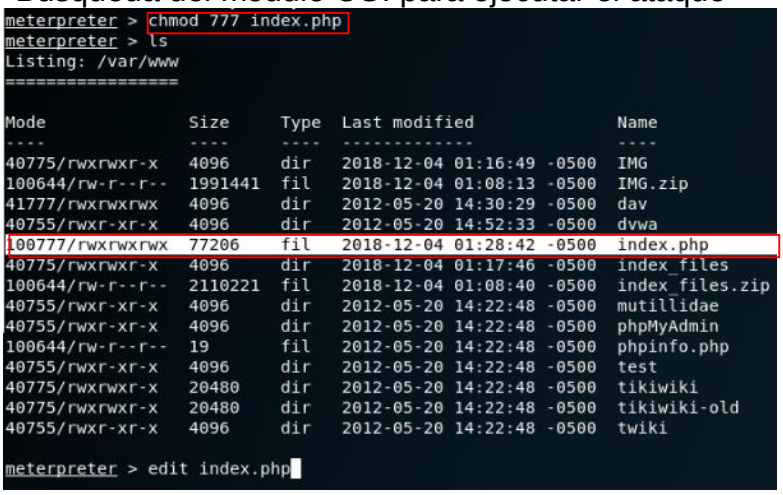
Figura 56. Ejecución de comandos remotos en el servidor vulnerable



Fuente: El autor

Inicialmente el Defacement consiste en modificar solo una parte de la página principal, por lo tanto, se ha identificado que el contenido estático está en el archivo ***index.php,*** sin embargo, el usuario ***www-data*** no cuenta con los permisos suficientes para editarlo. En Linux es posible establecer niveles de privilegios para acceder a un archivo o directorio según el propietario, miembros de un grupo o el resto de usuarios del sistema; esto añade una capa de seguridad por medio del control de acceso, no repudio y trazabilidad de las acciones realizadas por un determinado usuario. En la Figura 57 se procede a otorgar permisos administrativos de lectura, escritura y ejecución a través del comando ***chmod 777 index.php***.

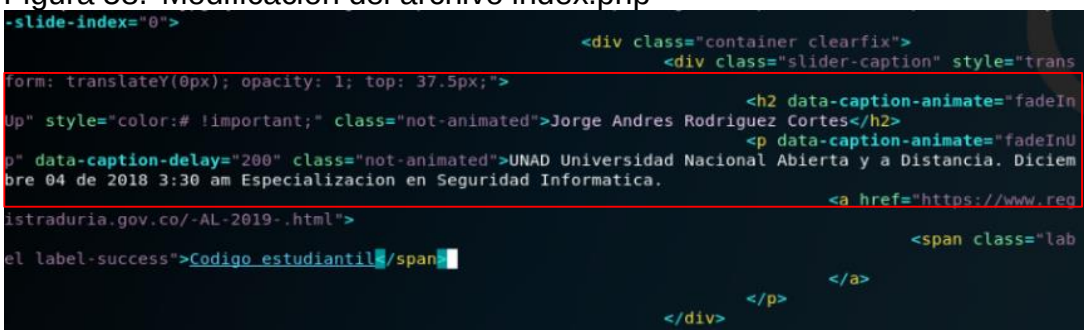
Figura 57. Búsqueda del módulo CGI para ejecutar el ataque



Fuente: El autor

Con los permisos asignados, se ejecuta el comando ***edit index.php*** y se cambian la información del banner por los datos personales del auditor. Esto es posible gracias al acceso obtenido al directorio ***/var/www***, ruta donde se almacenan todo el contenido web. En la Figura 58 se observa un fragmento del código de la página principal que ha sido modificado intencionalmente para observar la desfiguración parcial.

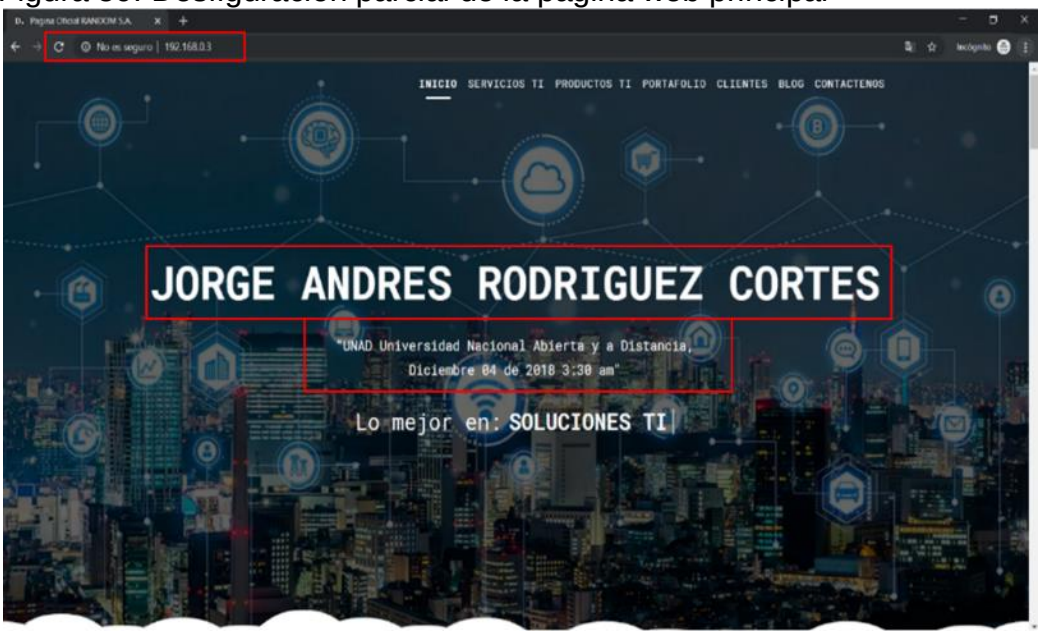
Figura 58. Modificación del archivo index.php



Fuente: El autor

Al consultar nuevamente la página principal se observa que su estructura permanece, sin embargo, el banner de bienvenida muestra la información del auditor y la modificación no autorizada del contenido. En la Figura 59 se observa la desfiguración parcial de la página principal, resaltando la hora y fecha de materialización del ataque.

Figura 59. Desfiguración parcial de la página web principal



Fuente: El autor

Hasta este punto se observa un cambio significativo en la página de Ramdom S.A., pero de cierto modo, su diseño prevalece. Esta modalidad puede ser usada por un atacante para alterar sutilmente el contenido de un sitio web e incrustar código malicioso que infecte con malware a los visitantes o redirigida a sitios de *Phishing*. Para realizar el Defacement por completo, en primera instancia se guarda una copia de respaldo de la página original por medio del comando de *meterpreter* ***download index.php***; una buena práctica es tomar evidencias de la configuración y respaldo de seguridad antes de llevar a cabo cualquier tipo de prueba de intrusión. En la Figura 60 se aprecia que el archivo descargado se almacena en la carpeta ***home*** de la maquina Kali Linux***.***

Figura 60. Descargar el código fuente original de la pagina

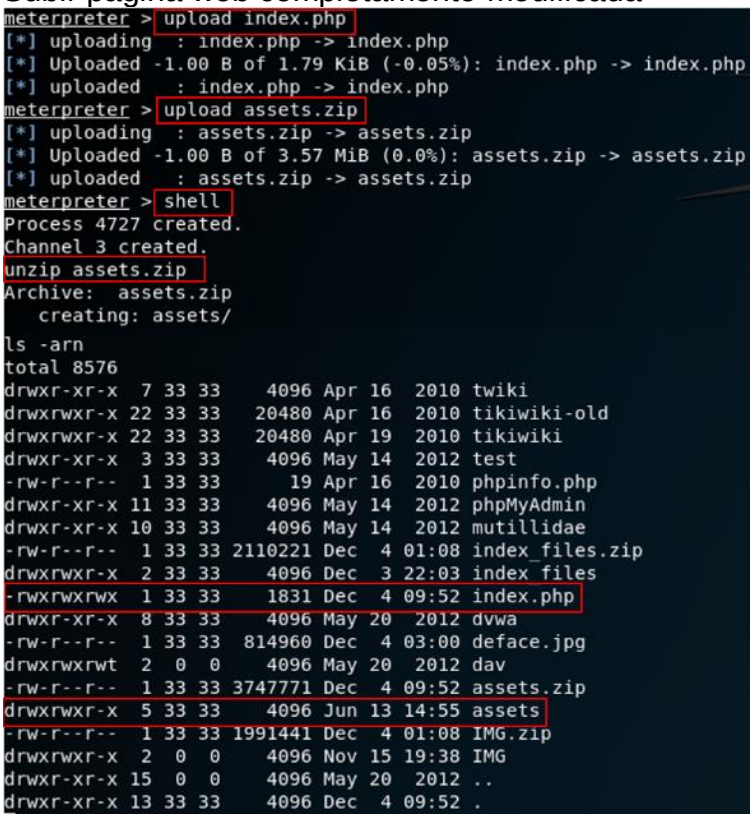
```
meterpreter > download index.php
[*] Downloading: index.php -> index.php
[*] Downloaded 75.36 KiB of 75.36 KiB (100.0%): index.php -> index.php
[*] download   : index.php -> index.php
meterpreter >
```

Fuente: El autor

Previamente se configuró una página web completamente modificada con sus correspondientes archivos complementarios como hojas de estilos e imágenes. En la Figura 61 se usa el comando ***upload index.php*** y ***upload***

assets.zip para subir y sobrescribir los archivos locales que están almacenados en el servidor web. Se observa que el archivo principal de la página web, ***index.php,*** ha sido sobrescrito, para que la pagina suplantada se visualice correctamente, se debe descomprimir el archivo ***assets.zip*** que tiene los archivos adicionales como hojas de estilo e imágenes.

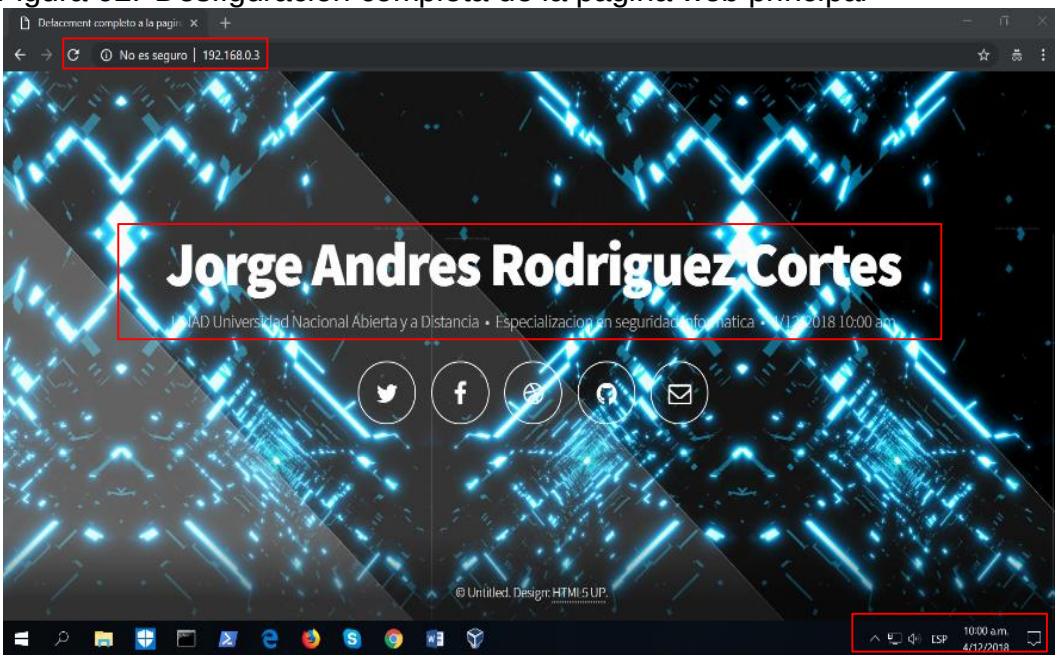
Figura 61. Subir página web completamente modificada



Fuente: El autor

Un *Defacement* tiene como finalidad afectar la integridad y disponibilidad de la información publicada en un aplicativo web, este tipo de ataques tiene motivación de índole económica, política, activista o personal. Una desfiguración impacta seriamente la imagen y la marca de una compañía, generando un daño considerable a la reputación. Al realizar nuevamente la consulta a la página principal, se observa que la estructura visual ha sido modificada completamente, mostrando la información del auditor y otra interfaz gráfica. En concordancia con el ataque del escenario I, en la Figura 62 se observa que la hora y fecha de la página coinciden con la configuración horaria del Host anfitrión, donde se realiza la petición web.

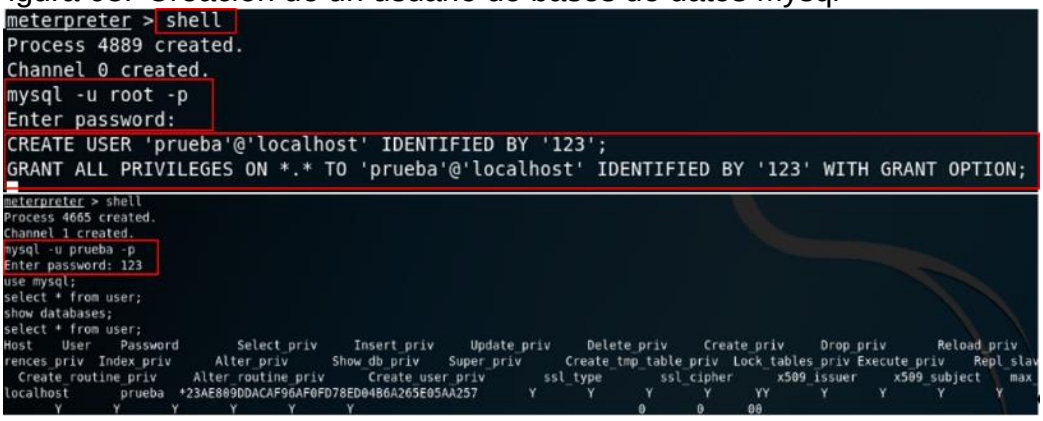
Figura 62. Desfiguración completa de la página web principal



Fuente: El autor

Otra acción interesante que se puede realizar con este ataque informático es levantar una ***shell*** de comandos a través de Meterpreter y aprovechar que el usuario ***root*** de Mysql no tiene contraseña, para de este modo, autenticarse y crear un usuario con privilegios de administrador en el módulo phpMyAdmin. En la Figura 63 se evidencia la creación del usuario ***prueba*** con permisos elevados para ingresar al módulo de bases de datos.

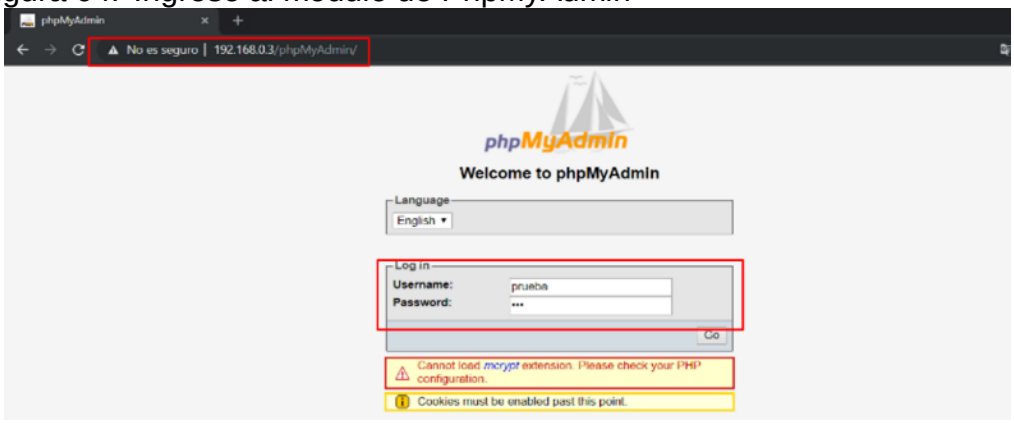
Figura 63. Creación de un usuario de bases de datos Mysql



Fuente: El autor

En la Figura 64 se muestra el ingreso al módulo ***phpMyAdmin*** mediante la interfaz web; se realiza la autenticación con el usuario creado de manera no autorizada y con las credenciales definidas en el paso anterior.

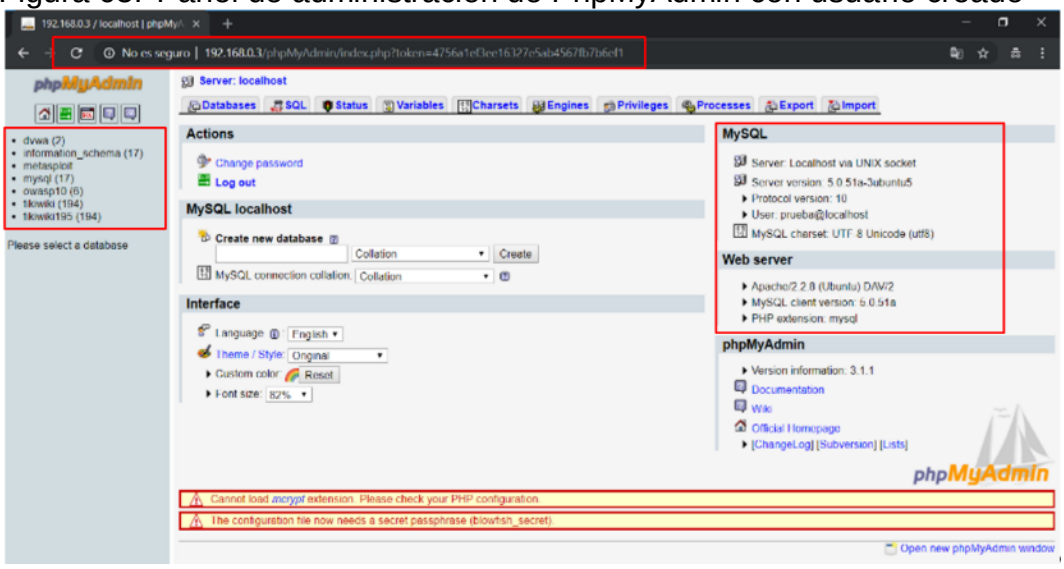
Figura 64. Ingreso al módulo de PhpMyAdmin



Fuente: El autor

En la Figura 65 se observa la página principal del módulo ***phpMyAdmin*** con la autenticación del usuario ***prueba***, el cual puede ejecutar consultas SQL a las bases de datos como crear, leer, modificar o eliminar.

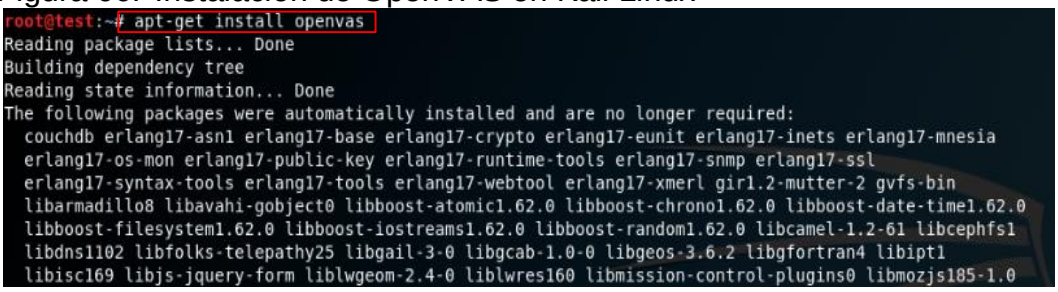
Figura 65. Panel de administración de PhpMyAdmin con usuario creado



Fuente: El autor

• **Instalación y configuración de OpenVAS.** Esta herramienta es un *framework* automatizado para ejecutar pruebas, análisis y detección de fallos de seguridad con base en vulnerabilidades identificadas en el listado NVD de la NIST (*National Institute of Standards and Technology*). En la Figura 66 se muestra la instalación de OpenVAS digitando el comando ***apt-get install openvas***. este proceso varía dependiendo de los recursos fiscos de la máquina y la velocidad de conexión hacia internet.

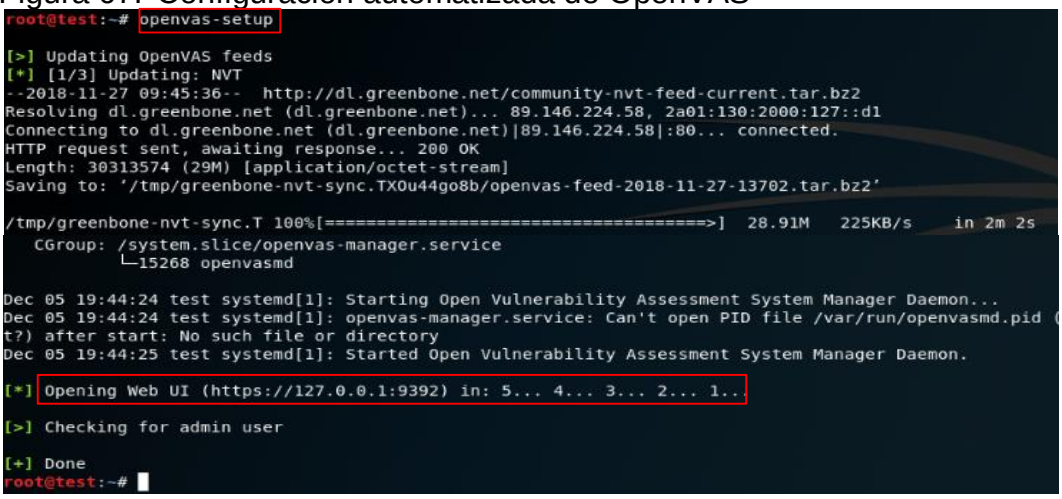
Figura 66. Instalación de OpenVAS en Kali Linux



Fuente: El autor

Al finalizar la instalación, se debe configurar OpenVAS por medio del comando ***openvas-setup***, después de este proceso se abre el navegador web y muestra la interfaz gráfica**.** En la Figura 67 se observa la configuración y puesta en marcha de los servicios de OpenVAS.

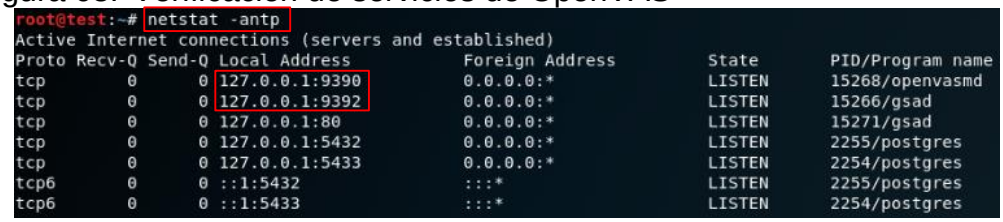
Figura 67. Configuración automatizada de OpenVAS



Fuente: El autor

Usando el comando ***netstat –antp*** se verifica que los puertos de OpenVAS están habilitados y activos en la máquina local. En la Figura 68 se evidencia que los puertos usados son el 9390 y 9392.

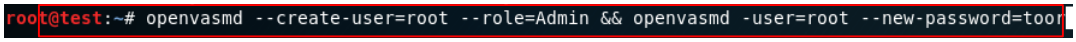
Figura 68. Verificación de servicios de OpenVAS



Fuente: El autor

Con la configuración de OpenVAS realizada satisfactoriamente, se procede a crear un usuario con privilegios para ingresar, debido a que el usuario por defecto *admin,* no funciona adecuadamente. En la Figura 69 se observa la creación de un usuario de OpenVAS por medio del comando ***openvasmd --create-user=root --role=Admin && openvasmd -user=root --new-password=toor.***

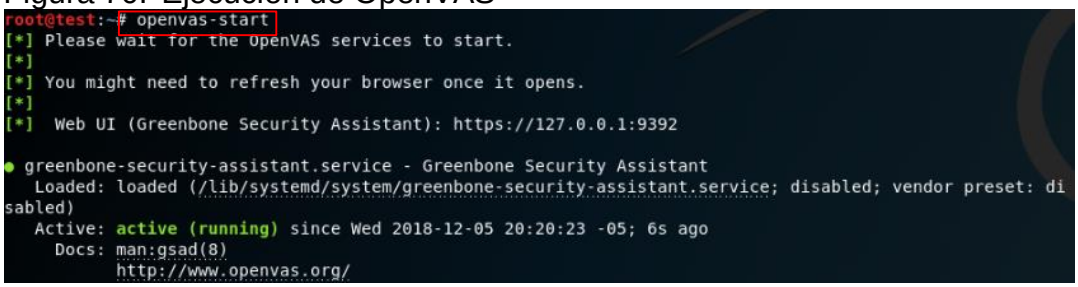
Figura 69. Creación de un usuario administrador en OpenVAS



Fuente: El autor

En la Figura 70 se aprecia el inicio de OpenVAS usando el comando ***openvas-start***. Al finalizar el proceso de carga de los módulos, el aplicativo se abre automáticamente en el navegador web.

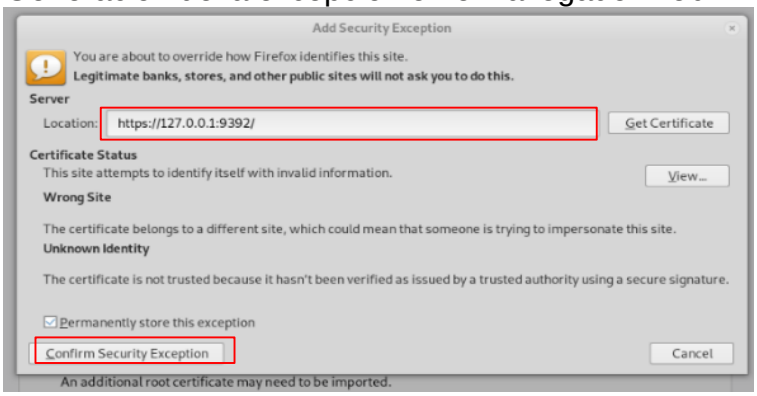
Figura 70. Ejecución de OpenVAS



Fuente: El autor

La primera vez que abre OpenVAS, lo hace por medio de la URL https://127.0.0.1:9392, sin embargo, se debe hacer una excepción en el navegador web permitiendo el acceso a la interfaz gráfica. En la Figura 71 se observa la confirmación de la excepción por falta de certificado.

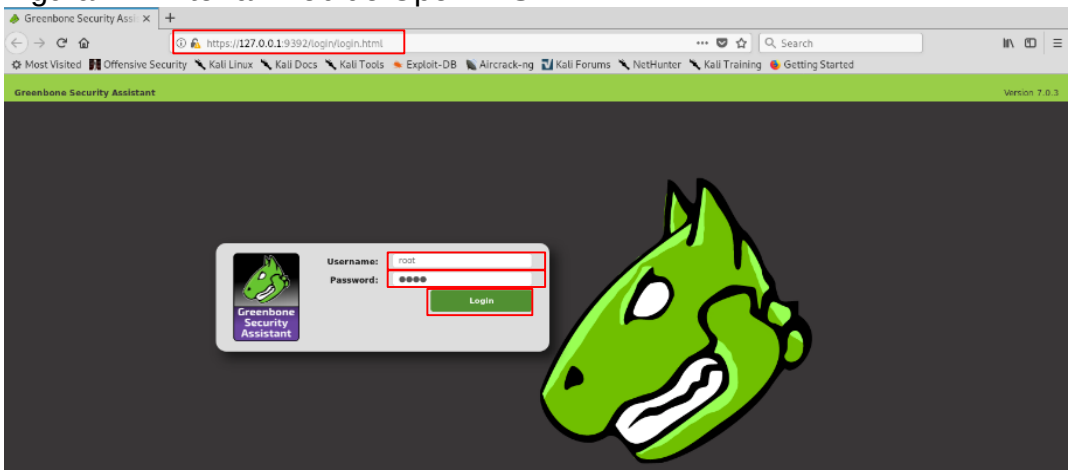
Figura 71. Generación de la excepción en el navegador web



Fuente: El autor

En la Figura 72 se aprecia la interfaz gráfica basada en web de OpenVAS. Para el inicio de sesión se utilizan las credenciales de acceso previamente creadas y se oprime el botón ***Login***.

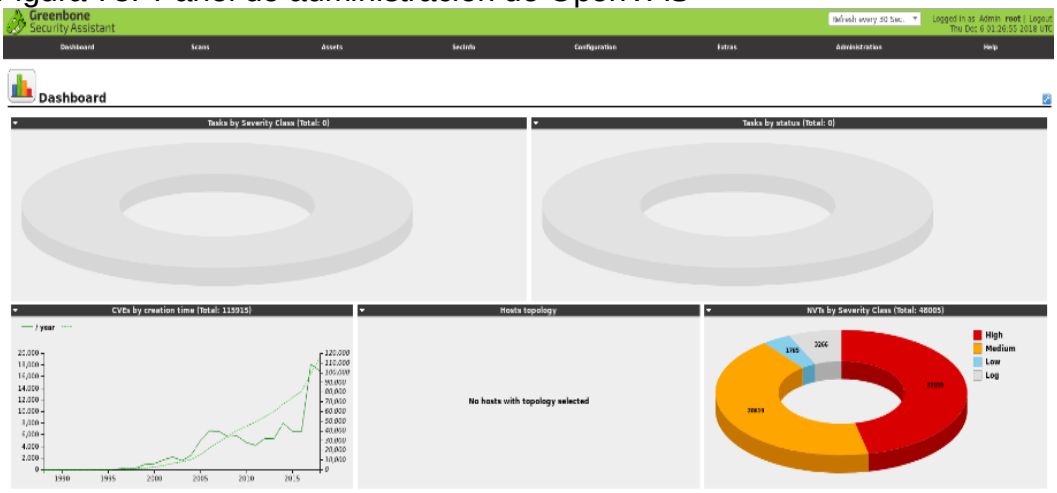
Figura 72. Interfaz web de OpenVAS



Fuente: El autor

En la Figura 73 se muestra el panel de administración de OpenVAS que permite la interacción con la herramienta. Existe un menú de opciones donde es posible configurar escaneos y realizar reportes.

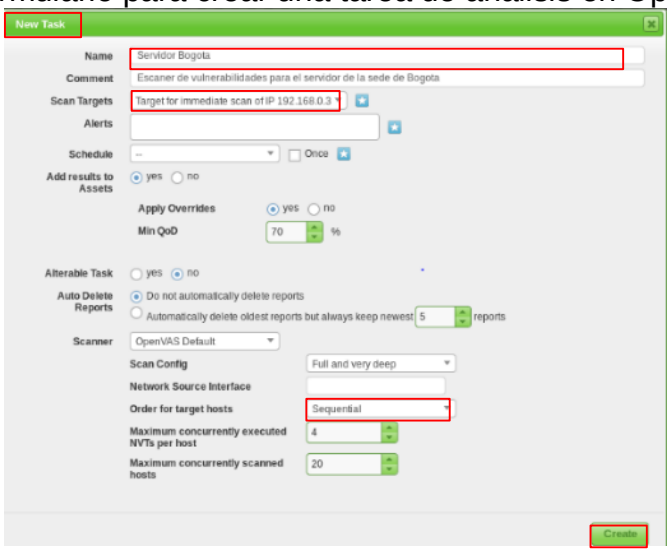
Figura 73. Panel de administración de OpenVAS



Fuente: El autor

- **Análisis de OpenVAS escenario 1.** Para ejecutar el escaneo de vulnerabilidades sobre una máquina, se debe ir al menú superior de OpenVAS y en la opción *Scans* >> *Task* >> *New Wizard* aparece un formulario donde se diligencian los parámetros del escaneo después *se* debe oprimir el botón *Create.*

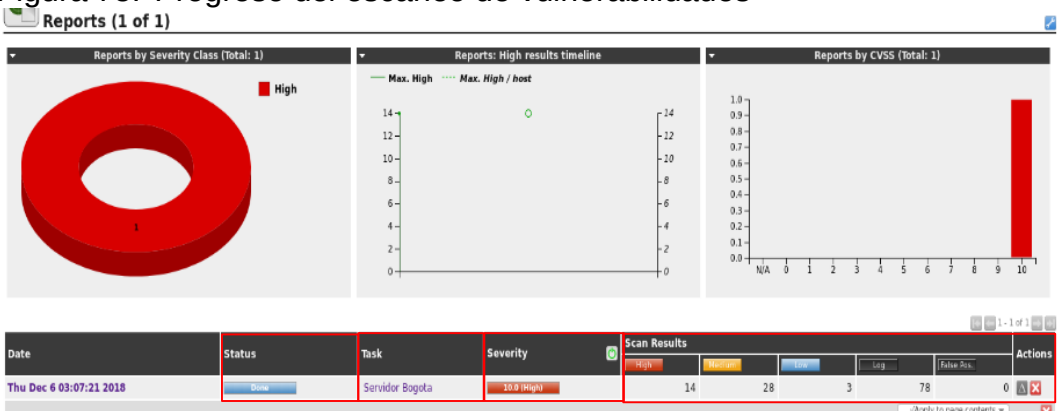
Figura 74. Formulario para crear una tarea de análisis en OpenVAS



Fuente: El autor

Después de configurar la opción más conveniente para la ejecución del test de vulnerabilidades, en la Figura 75 se muestra el progreso del escaneo de vulnerabilidades y los hallazgos encontrados hasta ese punto.

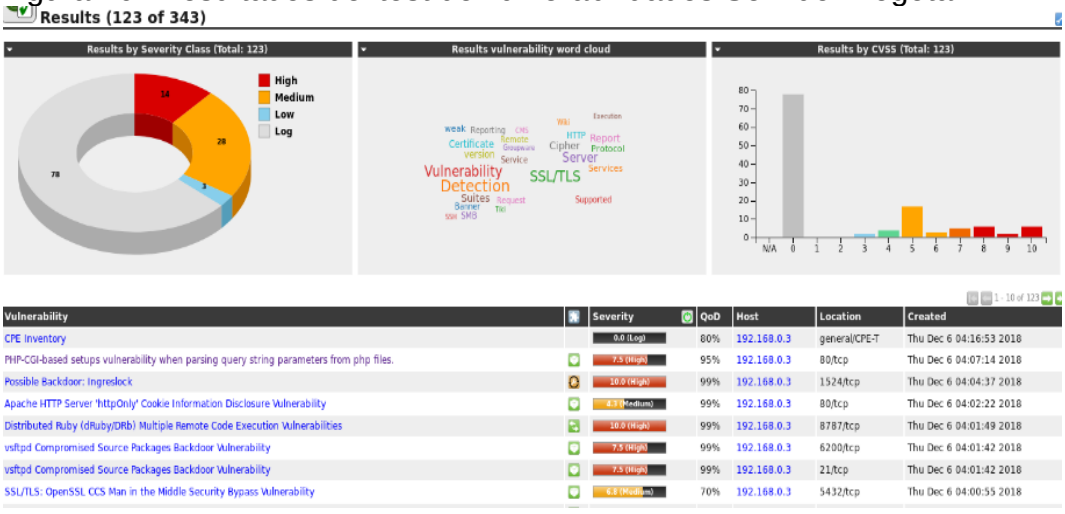
Figura 75. Progreso del escaneo de vulnerabilidades



Fuente: El autor

Para el servidor de Bogotá se encontraron 14 vulnerabilidades críticas, 29 con nivel medio, 3 con nivel bajo y 78 archivos de *logs* analizados. Adicionalmente, en la Figura 76 se evidencia que, en términos generales, el servidor del escenario I presenta estado crítico por múltiples vulnerabilidades y debe ser intervenido de manera inmediata.

Figura 76. Resultados del test de vulnerabilidades Servidor Bogotá



Fuente: El autor

OpenVAS cuenta con diferentes modos para visualizar los resultados obtenidos durante la ejecución del test de vulnerabilidades. En la Figura 77 se observan el listado de vulnerabilidades detectadas en aplicaciones conocidas como ***Apache server 2.2.8, PHP 5.2.4, PostgreSQL 8.3.1, phpMyAdmin 3.1.1, OpenSSH 4.7, ProFTPd 1.3.1***, entre otras.

Figura 77. Listado de vulnerabilidades detectadas del escenario I

Application CPE	Hosts	Occurrences	Severity
cpe:/a:apache:http_server:2.2.8	1	1	N/A
cpe:/a:php:php:5.2.4	1	1	N/A
cpe:/a:postgresql:postgresql:8.3.1	1	1	9.0 (High)
cpe:/a:phpmyadmin:phpmyadmin:3.1.1	1	1	4.3 (Medium)
cpe:/a:openbsd:openssh:4.7p1	1	1	N/A
cpe:/a:proftpd:proftpd:1.3.1	1	1	N/A
cpe:/a:x.org:x11:11.0	1	1	N/A
cpe:/a:postfix:postfix	1	1	N/A
cpe:/a:samba:samba:3.0.20	1	1	6.0 (Medium)
cpe:/a:beasts:vsftpd:2.3.4	1	1	N/A
cpe:/a:isc:bind:9.4.2	1	1	N/A
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5	1	1	7.5 (High)
cpe:/a:twiki:twiki:01.Feb.2003	1	1	10.0 (High)
cpe:/a:unrealircd:unrealircd:3.2.8.1	1	1	6.8 (Medium)

Port	IANA	Hosts	Severity
21/tcp		1	7.5
22/tcp		1	4.3
25/tcp		1	6.8
80/tcp		1	10.0
445/tcp		1	6.0
1099/tcp		1	10.0
1524/tcp		1	10.0
3632/tcp		1	9.3
5432/tcp		1	9.0
5900/tcp		1	9.0
6200/tcp		1	7.5
6667/tcp		1	6.8
8787/tcp		1	10.0

Fuente: El autor

OpenVAS ofrece una ficha técnica relacionada con cada una de las vulnerabilidades detectadas. Para acceder a esta información se debe hacer doble clic sobre la vulnerabilidad o código CVE. En la Figura 78 se muestra a manera de ejemplo la vulnerabilidad ***CVE-2012-1823 PHP-GCI-based setups vulnerability.***

Figura 78. Información de OpenVAS sobre una vulnerabilidad

Fuente: El autor

Un listado con mayor detalle se observa en la Figura 79, especificando el nombre de la vulnerabilidad, la severidad, puerto asociado y porcentaje de detección (QoD).

Figura 79. Listado de vulnerabilidades encontradas en el servidor Bogotá

Vulnerability	Severity	QoD	Host	Location	Actions
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.0.3	80/tcp	
OS End Of Life Detection	10.0 (High)	80%	192.168.0.3	general/tcp	
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95%	192.168.0.3	1099/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.0.3	8787/tcp	
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.0.3	1524/tcp	
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.0.3	3632/tcp	
PostgreSQL weak password	9.0 (High)	99%	192.168.0.3	5432/tcp	
VNC Brute Force Login	9.0 (High)	95%	192.168.0.3	5900/tcp	
phpinfo() output Reporting	7.5 (High)	80%	192.168.0.3	80/tcp	
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.0.3	80/tcp	
Test HTTP dangerous methods	7.5 (High)	99%	192.168.0.3	80/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.0.3	6200/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.0.3	21/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95%	192.168.0.3	80/tcp	
TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.8 (Medium)	80%	192.168.0.3	80/tcp	
UnrealIRCd Authentication Spoofing Vulnerability	6.8 (Medium)	80%	192.168.0.3	6667/tcp	
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	6.8 (Medium)	99%	192.168.0.3	25/tcp	
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Medium)	70%	192.168.0.3	5432/tcp	
Anonymous FTP Login Reporting	6.4 (Medium)	80%	192.168.0.3	21/tcp	
TWiki Cross-Site Request Forgery Vulnerability	6.0 (Medium)	80%	192.168.0.3	80/tcp	
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	6.0 (Medium)	99%	192.168.0.3	445/tcp	
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99%	192.168.0.3	80/tcp	
Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability	5.0 (Medium)	80%	192.168.0.3	80/tcp	
SSL/TLS: Certificate Expired	5.0 (Medium)	99%	192.168.0.3	25/tcp	
SSL/TLS: Certificate Expired	5.0 (Medium)	99%	192.168.0.3	5432/tcp	
/doc directory browsable	5.0 (Medium)	80%	192.168.0.3	80/tcp	
Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability	5.0 (Medium)	80%	192.168.0.3	80/tcp	
awiki Multiple Local File Include Vulnerabilities	5.0 (Medium)	99%	192.168.0.3	80/tcp	
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80%	192.168.0.3	80/tcp	
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	4.3 (Medium)	80%	192.168.0.3	25/tcp	
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	192.168.0.3	5432/tcp	
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	192.168.0.3	25/tcp	
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)	4.3 (Medium)	80%	192.168.0.3	25/tcp	
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.0.3	5432/tcp	
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.0.3	22/tcp	
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	192.168.0.3	5432/tcp	
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	192.168.0.3	25/tcp	
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	4.3 (Medium)	99%	192.168.0.3	80/tcp	
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4.3 (Medium)	99%	192.168.0.3	80/tcp	
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80%	192.168.0.3	5432/tcp	
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80%	192.168.0.3	25/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	192.168.0.3	5432/tcp	
Tiki Wiki CMS Groupware XSS Vulnerability	3.5 (Low)	80%	192.168.0.3	80/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.0.3	general/tcp	
SSH Weak MAC Algorithms Supported	2.6 (Low)	95%	192.168.0.3	22/tcp	

Fuente: El autor

En el Cuadro 5 se encuentra registrada la descripción de las vulnerabilidades con mayor nivel de riesgo para el servidor de la sede Bogotá, según el CVSS (*Common Vulnerability Score System*).

Cuadro 5.Top de vulnerabilidades encontradas en el servidor de Bogotá

Código CVE	Descripción	CVSS	Producto afectado
CVE-2010-0425	Permite a un atacante la ejecución de código remoto por medio de una llamada al módulo ISAPI que contiene código vulnerable.	10	Apache server 2.2.8
CVE-2008-0122	Permite denegación de servicio y ejecución remota de código aprovechando una entrada del buffer de memoria.	10	Bind 9.4.2
CVE-2012-1667	Manejo inadecuado de registros que ocasión una denegación de servicio ocasionada por servidores DNS.	8.5	Bind 9.4.2
CVE-2012-1823	Es una vulnerabilidad que permite la ejecución de un script PHP –CGI para la ejecución de código remoto. Se trata de un manejo deficiente en las cadenas de consulta	7.5	PHP 5.2.4
CVE-2008-0599	No toma en cuenta la prioridad de un operador cuando se realiza el cálculo de la longitud, permitiendo la ejecución de código remoto.	10	PHP 5.2.4
CVE-2008-2050	Desbordamiento de Buffer en la pila FastCGI, impacto desconocido.	10	PHP 5.2.4
CVE-2008-5557	Permite la ejecución de código remoto por medio de una cadena Unicode que no ha sido manejada en un archivo HTML.	10	PHP 5.2.4
CVE-2009-4143	Manejo inadecuado de los datos de sesión, impacto desconocido.	10	PHP 5.2.4
CVE-2011-3268	Desbordamiento de buffer en la función de HASH, impacto desconocido.	10	PHP 5.2.4
CVE-2012-2376	Desbordamiento de buffer en la función de com_print_typeinfo, permite ejecutar código remotamente.	10	PHP 5.2.4
CVE-2012-2688	Vulnerabilidad en la función php_stream, impacto desconocido.	10	PHP 5.2.4
CVE-2007-1581	Vulnerabilidad en la función hash_update, afecta los recursos y permite ejecutar código remotamente.	9.3	PHP 5.2.4
CVE-2013-1902	Generación de archivos temporales poco seguros, impacto desconocido.	10	PostgreSQL 8.3.1
CVE-2016-7048	Ejecución de código remoto por medio del instalador de PostgreSQL que se descarga vía HTTP.	9.3	PostgreSQL 8.3.1
CVE-2010-1168	Omisión de acceso seguro y escalamiento de privilegios por medio de llamada a métodos Destroy() y AutoLoad().	7.5	PostgreSQL 8.3.1
CVE-2010-1447	Ejecución de código remoto por medio de referencias y subrutinas vulnerables.	8.5	PostgreSQL 8.3.1
Fuente: El autor, basado en *Common Vulnerabilities and Exposures*.			

• **Planteamiento de la DMZ.** Las organizaciones utilizan Internet como un medio para ofrecer productos y servicios, lo cual es a fin con el negocio, sin embargo, esto crea una apertura entre la red privada y la red pública dejando expuesta la información a múltiples riesgos. “Debido a esto es necesario establecer una zona segura y aislada en la cual se publiquen los recursos y contenidos que posteriormente serán accedidos por usuarios de todo el mundo, tal zona se encuentra ubicada entre la red interna LAN y una red externa que puede ser una red WAN o Internet”[62].

En la zona desmilitarizada (DMZ) se debe garantizar que los recursos y/o servicios están disponibles, es decir, no debe tener restricciones o bloqueos, sin embargo, para asegurar los activos de la información privados tampoco se puede tener acceso desde esta zona a la red interna de la organización. En ese sentido, las conexiones desde Internet y la red interna hacia la DMZ están permitidas para efectos de acceso y administración respectivamente, pero las conexiones desde la DMZ hacia la red interna están restringidas.

El uso habitual para la DMZ es albergar servidores en los cuales se publica algún tipo de servicio que debe ser consumido desde una red externa, por ejemplo: una página web (WWW), transferencia de archivos (FTP), resolución de nombres de dominio (DNS), correo electrónico (SMTP), entre otros. Para el planteamiento de la DMZ se propone utilizar una arquitectura de red perimetral compuesta por 2 Firewall en los cuales se define una zona interna para los servicios privados y una zona desmilitarizada para las publicaciones.

- **Zona desmilitarizada**: En esta zona están localizados los servicios y aplicaciones que se ofrecen a redes externas. Para fortalecer la seguridad en esta zona se utilizan dispositivos especializados como Firewall para aplicaciones web, Anti-DDoS, *Honey Pot* y soluciones de antivirus y *Endpoint*. El objetivo de la DMZ es aislar la red corporativa de las peticiones que provienen de Internet. El tráfico desde la red interna y externa hacia la DMZ está permitido, no se permite ningún tipo de trafico de salida y cualquier otro tipo de comunicación será denegada.

- **Zona interna**: En esta zona se ubican las estaciones de trabajo, servicios y aplicaciones de carácter organizacional. En esta red privada la seguridad se adopta el modelo por capas, donde intervienen dispositivos tecnológicos, políticas, técnicas, tácticas y procedimientos para proteger la privacidad de la información corporativa. Solo se permite el tráfico de

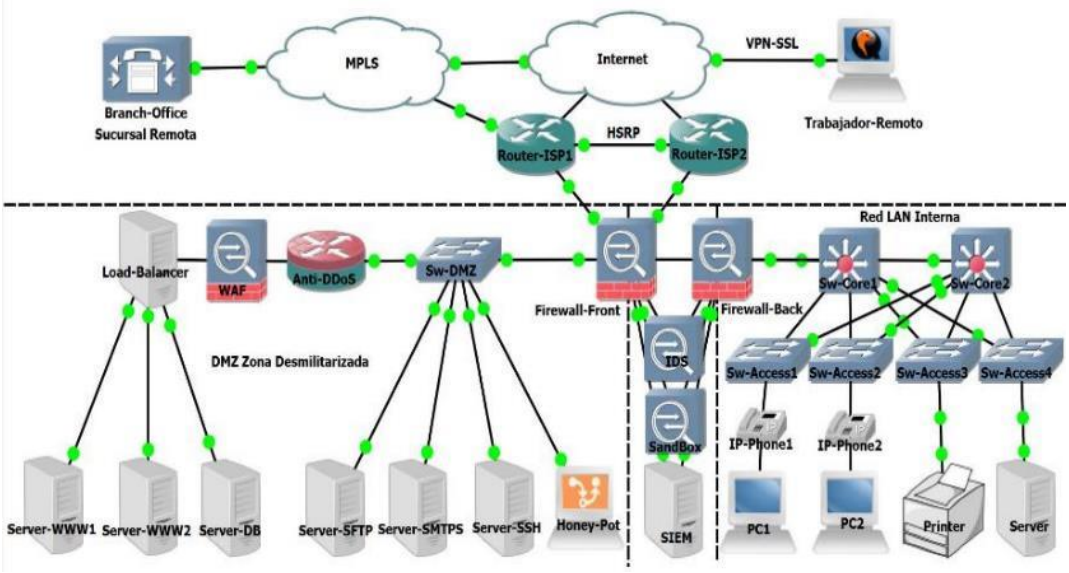
[62] ESPAÑA, Instituto Nacional de Ciberseguridad. Qué es una DMZ y cómo te puede ayudar a proteger tu empresa [En línea], 2019. [Citado el 25 de noviembre de 2098]. Disponible en Internet: < https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa >.

salida desde la red interna hacia la DMZ y la red externa, además no se permite ningún tipo de petición de entrada hacia la red interna.

- **Zona externa**: Esta zona es habitualmente referenciada con Internet y es el lugar en el ciberespacio donde se producen todo tipo de interacciones digitales. Por ser una zona publica y con diferentes administraciones, carece de seguridad, privacidad y es utilizada para desarrollar campañas maliciosas de manera anónima. A nivel de seguridad en esta zona, se utilizan redes privadas virtuales y cifrado de los datos que viajan por el medio inseguro.

En cuanto a arquitectura, la red corporativa debe estar segmentada e incluir equipos activos que protejan la información de cada uno de los nodos. En la Figura 80 se presenta la propuesta de topología para la red corporativa en la sede Bogotá.

Figura 80. Topología de red para la empresa RANDOM S.A. - Bogotá



Fuente: El autor

- **Políticas de seguridad.** La Empresa RANDOM S.A. se ha comprometido con la definición de lineamientos y disposiciones de alto nivel, que tienen finalidad de garantizar y proteger la confidencialidad, integridad y disponibilidad de la información propia, de clientes, de colaboradores y de terceros; la cual es requerida para la correcta operación del negocio en cumplimiento de su visión, misión y objetivos estratégicos.

La presente política aplica de manera transversal para todos los recursos tecnológicos de RANDOM S.A. y es de carácter obligatorio su cumplimiento de parte de todos los usuarios que tengan algún tipo de vínculo con los activos de la información.

- **Copias de respaldo de información**: Realizar y mantener copias de respaldo según lo dispuesto en el procedimiento de restauración de información, para de este modo recuperar los sistemas de información en caso de cualquier tipo de falla. Además de establecer las pruebas de restauración periódicamente con el fin de garantizar la efectividad de esta actividad. Las copias de seguridad se realizan según el rol del activo, esto quiere decir que para servidores se ejecuta la tarea automática de respaldo dependiendo la criticidad del activo, (mensual, semanal o a diario). Para estaciones de trabajo es responsabilidad del colaborador realizar la solicitud según lo crea conveniente.

  Las copias de respaldo son almacenadas localmente en el servidor NAS (*Network Attached Storage*) de la organización durante un periodo de 3 meses, posteriormente son llevas a un servicio de almacenamiento en la nube. Para restablecer una copia de seguridad, es necesario formalizar el tramite a través de un correo enviado al área de sistemas con copia al jefe inmediato del colaborador que está realizando la solicitud.

- **Inventario de activos:** Todos los activos tecnológicos deben tener asignado un propietario, quien será el encargado de la administración del mismo y responderá durante el ciclo de vida del activo, adicionalmente, se debe asegurar que los activos de información se encuentren inventariados, identificados y que sean propiamente clasificados y etiquetados, conforme con las directrices de la compañía.

  Toda la información que la organización considere como sensible o critica, al igual que los activos a través de los cuales es procesada o almacenada, deberán ser inventariados, contar con un responsable asignado, estar clasificados para determinar su nivel de acceso y los procedimientos para su manipulación, además de darles tratamiento siguiendo los lineamientos estipulados por la gerencia de RANDOM S.A.

- **Manejo de la Información y disposición de recursos tecnológicos:** Todo funcionario que labore en RANDOM S.A. y utilice sus recursos tecnológicos, tiene la obligación de preservar la integridad, confidencialidad, disponibilidad y confiabilidad de toda información que sea considerada como crítica, privilegiada o se encuentre protegida por reserva legal. Así mismo, no deberá suministrar, comercializar o divulgar información empresarial a ningún organismo externo sin que previamente

se le hayan concedido los permisos respectivos. Todos los dispositivos y medios tecnológicos donde se crea, procesa, transmite y almacena información de la empresa deben mantenerse bajo las medidas de protección físicas y lógicas.

- **Aplicación de actualizaciones o cambios en la configuración**: Deben ser ejecutados inicialmente en un ambiente de pruebas, en el evento de no estar disponibles los parches o los resultados de las pruebas no son satisfactorios, se deben utilizar controles compensatorios. El sistema operativo con el cual trabaja un servidor debe estar diseñado para cumplir este fin, por lo tanto, se establece solo el uso de sistemas operativos tipo servidor para los equipos que ofrecen cualquier servicio en la entidad, además tal sistema operativo debe contar con todas las actualizaciones, las cuales se ejecutan regularmente la primera semana del mes a una hora definida por el área de Sistemas.

- **Dispositivos de seguridad perimetral**: La información que maneja la empresa RANDOM S.A. es importante y critica para las operaciones del negocio, por lo tanto, se establece la implementación de dispositivos activos especializados en proteger la información, como Firewall, anti-DDoS, WAF, balanceador de cargas, entre otros. Todas las conexiones a redes externas de tiempo real que accedan a la red interna de RANDOM S.A., deben ser autorizadas por el área de Sistemas y están obligadas a pasar por los sistemas de seguridad perimetral dispuestos por la empresa (servicios de cifrado y verificación de datos, administración de permisos de usuarios y demás controles tecnológicos que se consideren pertinentes).

- **Control de acceso a código fuente de aplicativos**: El código fuente de los aplicativos misionales debe estar completamente restringido para todo tipo de usuarios sin autorización y controlado para usuarios con permisos de acceso, la aplicación de ingeniería inversa está prohibida. Deben establecerse medidas de control de acceso en los diferentes niveles de la plataforma tecnológica de la organización como lo son dispositivos de red, sistemas operativos y aplicaciones, para permitir el acceso únicamente a los usuarios que por el desempeño de sus funciones estén directamente relacionados con la generación, uso y manipulación de la información.

- **Separación de ambientes de pruebas y producción**: Cualquier tipo de desarrollo o modificación en algún sistema informático de la organización debe ser probado bajo un ambiente controlado para su posterior despliegue a producción. Todos los cambios realizados en la plataforma tecnológica de RANDOM S.A. deben quedar debidamente

documentados, desde la solicitud realizada por el funcionario competente hasta su implementación, de manera que facilite su trazabilidad y permita dar seguimiento a los procedimientos establecidos.

- **Gestión de vulnerabilidades técnicas**: Se debe ejecutar un escaneo de vulnerabilidades quincenalmente o cuando exista un cambio significativo en la red o en los servidores críticos de la empresa. Este escaneo no intrusivo se debe realizar de manera planificada y cuidadosa para reducir el riesgo de interrupción o afectación en los servicios críticos de la organización. El resultado de las pruebas de vulnerabilidades debe ser reportado al responsable del activo e informado al área de Sistemas para llevar a cabo las acciones de contención y/o erradicación de la brecha de seguridad detectada.

- **Seguridad en las comunicaciones:** Toda la información clasificada como secreta, confidencial o crítica que se transmita por las redes de datos de RANDOM S.A., redes de datos de terceros e internet debe estar cifrada durante su almacenamiento y transmisión de forma que se evite su alteración o cambios en su estructura, evitando que puedan afectar su confidencialidad, disponibilidad e integridad. Únicamente debe estar en legible cuando sea consultada por los funcionarios o usuarios a través de la interfaz gráfica de usuario.

- **Contraseñas de acceso:** Las claves asignadas son personales e intransferibles, cualquier uso fraudulento de las mismas será responsabilidad de los funcionarios que las tienen a su cargo. La contraseña de acceso debe ser una combinación de letras, números, caracteres alfanuméricos y signos, que el usuario debe digitar para obtener acceso al sistema o al dominio de la empresa. Las contraseñas de ingreso a los sistemas de RANDOM S.A. deberán cambiarse periódicamente en un plazo no mayor a 60 días (política definida en el sistema de administración de usuarios).

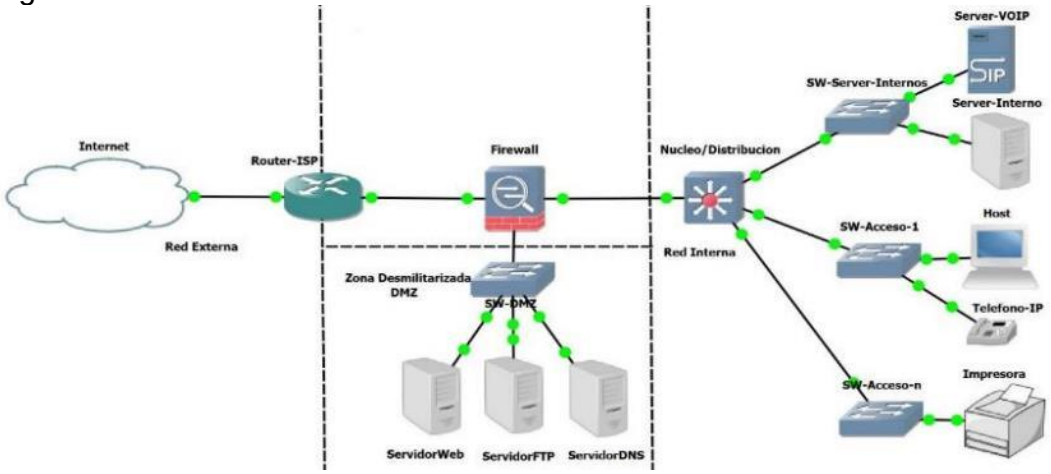
- **Mantenimiento preventivo y correctivo de equipos de cómputo:** Se debe garantizar la revisión y optimización del funcionamiento de todas las estaciones de trabajos, servidores e impresores de la empresa RANDOM S.A; para esto se llevan a cabo 2 brigadas en el año con el objetivo de mejorar el rendimiento de hardware y software, detectar y corregir fallos, prolongar la vida útil del dispositivo y generar la documentación correspondiente para el inventario de activos.

- **Desarrollo de sistemas de información:** Los sistemas informáticos de la organización soportan todos los requerimientos establecidos en las normativas de seguridad de la información, por lo tanto, estos

requerimientos deben ser considerados en cada paso del ciclo de desarrollo de software, incluyendo todas las fases de análisis, diseño, desarrollo, mantenimiento y operación.

- **Firewall de 3 interfaces.** Un firewall es un control tecnológico de tipo hardware o software que realiza el filtrado de paquetes en una red de datos, capaz de permitir, descartar, bloquear, modificar y convertir un datagrama IP. Existe un tipo de firewall que se caracteriza por tener 3 interfaces donde se establece 1 zona por cada interfaz; red externa, DMZ y red interna. Este esquema es el más básico de implementar, pero dependiendo de las configuraciones aplicadas en el firewall, un atacante puede usar algún puerto a la escucha para acceder a la red interna, por ende, es recomendable adicionar otra capa de seguridad. En la Figura 81 se presenta una topología de red basada en un firewall de 3 interfaces.

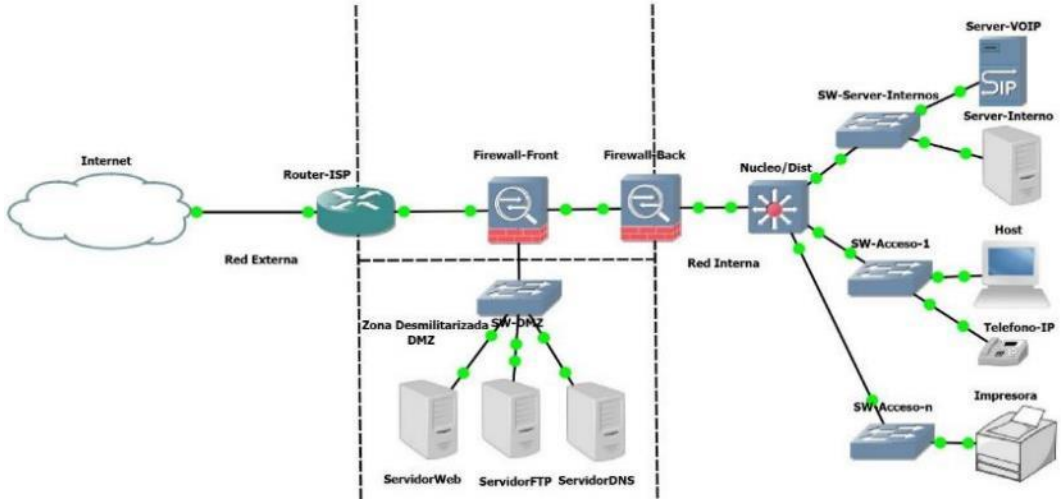
Figura 81. DMZ con un firewall de 3 interfaces



Fuente: El autor

- **Firewall screened-subnet.** Al igual que la anterior topología, se establecen 3 zonas, red externa, DMZ y red interna, pero la diferencia de esta topología radica en la implementación de 2 dispositivos de filtrado de paquetes. El primero, (*Front-End*), realiza una revisión inicial del tráfico y permite el tráfico hacia la DMZ y el segundo, (*Back-End*), realiza el filtrado riguroso de paquetes permitiendo el tráfico desde y hacia la red interna. Con esta opción se puede aplicar re-direccionamiento de puertos a través de PAT (*Port Address Translation*) para evitar que un usuario externo tenga información relevante de un recurso interno. En la Figura 82 se presenta una topología de red basada en 2 firewall y 3 zonas perimetrales.

Figura 82. DMZ con 2 firewall screened-subnet



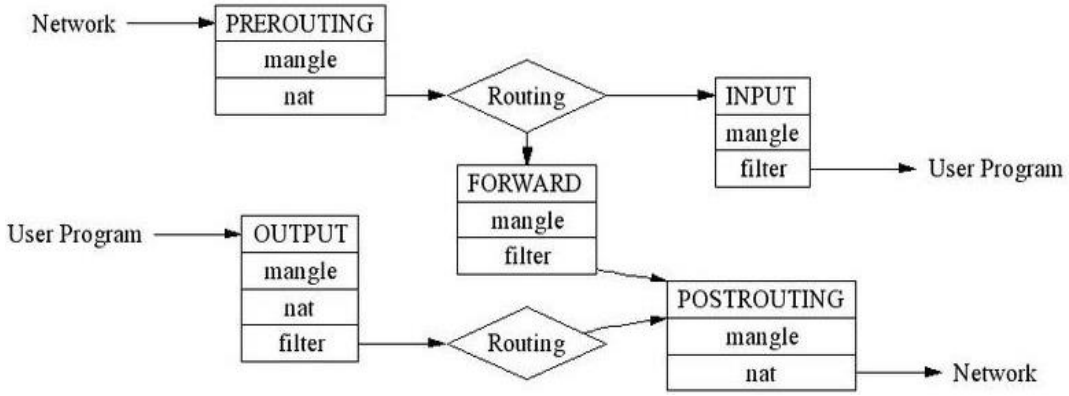
Fuente: El autor

• **Firewall por software.** IPTables es un firewall robusto incluido en el *kernel* de Linux que hace parte del proyecto *netfilter*, que permite ejecutar reglas en un conjunto de tablas y sus correspondientes cadenas que tienen una función definida. Es utilizado para el filtrado de paquetes, calidad de servicio y manejo de datagramas, además es posible establecer acciones como reenvío, modificación, redirección o eliminación de un paquete que ingresa por una interfaz de red. Los firewalls avanzados de nueva generación esta basados en IPTables por ser flexible, potente y confiable, además garantiza un nivel de seguridad óptimo para el tráfico y transporte de la red.

IPTables está basado en una colección de tablas (***Mangle - NAT - Filter***), que contienen cadenas establecidas bajo una secuencia lógica (***PreRouting – PostRouting – Input – Output - Forward***), con cada una de las cadenas se tiene un grupo de reglas asociado. "La Tabla ***Filter*** se encarga del filtrado y manejo de los paquetes, mientras que la Tabla ***NAT*** sirve para el reenvío de paquetes; por último, la Tabla ***mangle*** es la encargada de alterar las etiquetas, *flags,* de los paquetes"[63]. Cada datagrama IP enviado o recibido por la interfaz de red está sujeto por lo menos a una tabla, en la Figura 83 se observa el recorrido que debe realizar un paquete de datos cuando ingresa por un dispositivo que tiene configurado *IPTables*.

[63] RED HAT, Inc. 2.6. IPTABLES. [En línea]. [Citado el 25 de noviembre de 2018]. Disponible en Internet: <https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-iptables>.

Figura 83. Tipo de cadenas establecida en IPTables



Fuente: MOLINA, Alberto. Qué es iptables. [En línea], 2018. [Citado el 25 de noviembre de 2018]. Disponible en Internet: <https://openwebinars.net/blog/que-es-iptables/>.

Con base en lo anterior y como medida de prevención ante los ataques sufridos en el servidor de la sede principal de RANDOM S.A, se propone la configuración de un conjunto de reglas del firewall IPTables sobre la máquina Metasploitable 2 que cuenta con *kernel* de Linux. Inicialmente una distribución Linux no tiene definida ninguna política de filtrado, por lo tanto, antes de iniciar la configuración del firewall por software es necesario contar con permisos de súper usuario para configurar IPTables. En la Figura 84 se observa el proceso de verificación de reglas usando el comando ***sudo iptables -n -L -v --line-numbers***.

Figura 84. Verificación de IPTables antes de ingresar las reglas

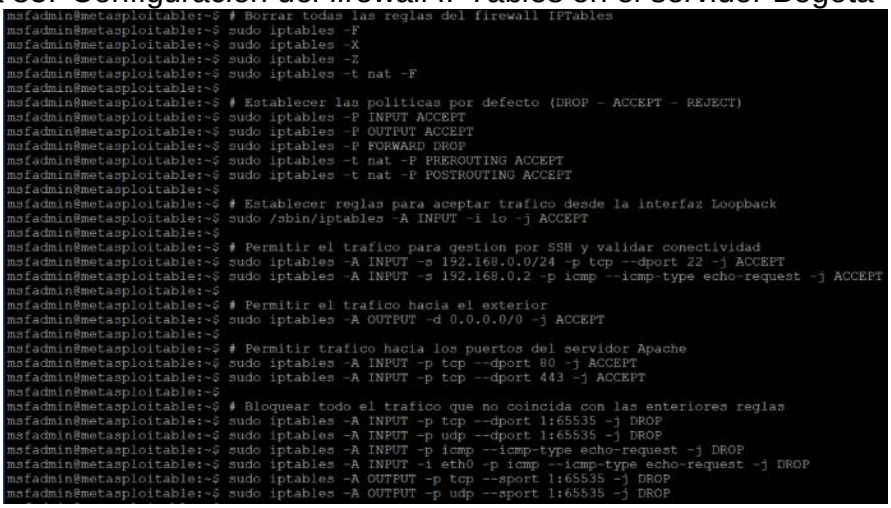
```
msfadmin@metasploitable:~$ sudo iptables -n -L -v --line-numbers
Chain INPUT (policy ACCEPT 1731 packets, 181K bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1581 packets, 113K bytes)
num   pkts bytes target     prot opt in     out     source               destination
```

Fuente: El autor

En la Figura 85 se presenta la edición del conjunto de reglas que deben ser aplicadas de manera secuencial en la maquina Metasploitable 2. En primera instancia se elimina cualquier tipo de registro previo para evitar solapamiento de reglas, después, se establecen las políticas por defecto las cuales dependen si el firewall tiene un enfoque permisivo o restrictivo. Vale la pena resaltar que esta configuración está diseñada en permitir

únicamente el tráfico web y la administración desde una red de confianza, para el resto de peticiones de salida o entrada se deniega la conexión.

Figura 85. Configuración del firewall IPTables en el servidor Bogotá

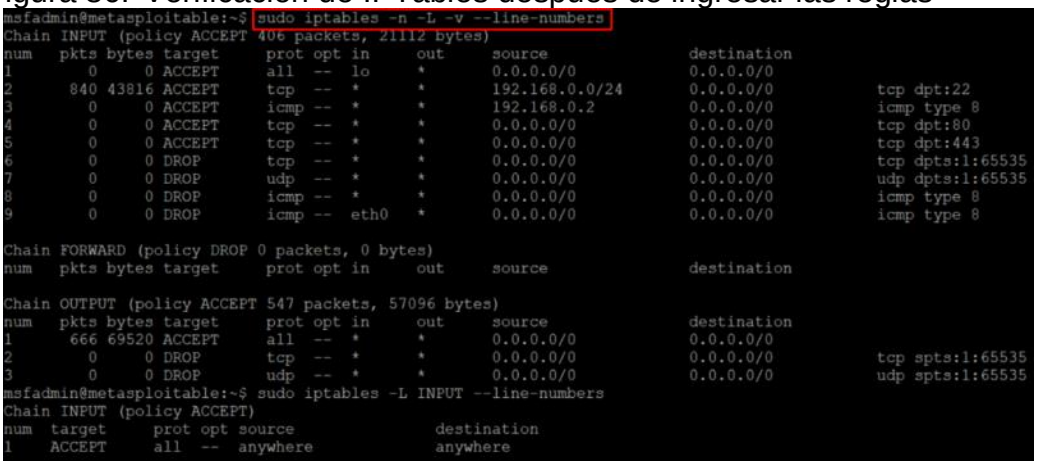


```
msfadmin@metasploitable:~$ # Borrar todas las reglas del firewall IPTables
msfadmin@metasploitable:~$ sudo iptables -F
msfadmin@metasploitable:~$ sudo iptables -X
msfadmin@metasploitable:~$ sudo iptables -Z
msfadmin@metasploitable:~$ sudo iptables -t nat -F
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ # Establecer las politicas por defecto (DROP - ACCEPT - REJECT)
msfadmin@metasploitable:~$ sudo iptables -P INPUT ACCEPT
msfadmin@metasploitable:~$ sudo iptables -P OUTPUT ACCEPT
msfadmin@metasploitable:~$ sudo iptables -P FORWARD DROP
msfadmin@metasploitable:~$ sudo iptables -t nat -P PREROUTING ACCEPT
msfadmin@metasploitable:~$ sudo iptables -t nat -P POSTROUTING ACCEPT
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ # Establecer reglas para aceptar trafico desde la interfaz Loopback
msfadmin@metasploitable:~$ sudo /sbin/iptables -A INPUT -i lo -j ACCEPT
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ # Permitir el trafico para gestion por SSH y validar conectividad
msfadmin@metasploitable:~$ sudo iptables -A INPUT -s 192.168.0.0/24 -p tcp --dport 22 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -s 192.168.0.2 -p icmp --icmp-type echo-request -j ACCEPT
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ # Permitir el trafico hacia el exterior
msfadmin@metasploitable:~$ sudo iptables -A OUTPUT -d 0.0.0.0/0 -j ACCEPT
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ # Permitir trafico hacia los puertos del servidor Apache
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ # Bloquear todo el trafico que no coincida con las enteriores reglas
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1:65535 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p udp --dport 1:65535 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -j DROP
msfadmin@metasploitable:~$ sudo iptables -A OUTPUT -p tcp --sport 1:65535 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A OUTPUT -p udp --sport 1:65535 -j DROP
```

Fuente: El autor

Al aplicar las reglas de IPTables se usa nuevamente el comando ***sudo iptables -n -L -v --line-numbers*** para validar el resultado del filtrado de paquetes. En la Figura 86 se aprecia que las configuraciones se aplicaron correctamente y dependiendo el sentido de la comunicación, se evalúa un paquete de manera secuencial en la Tabla correspondiente.

Figura 86. Verificación de IPTables después de ingresar las reglas

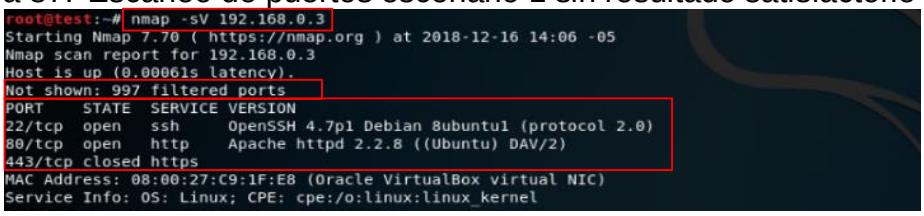


```
msfadmin@metasploitable:~$ sudo iptables -n -L -v --line-numbers
Chain INPUT (policy ACCEPT 406 packets, 21112 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
2      840 43816 ACCEPT     tcp  --  *      *       192.168.0.0/24       0.0.0.0/0           tcp dpt:22
3        0     0 ACCEPT     icmp --  *      *       192.168.0.2          0.0.0.0/0           icmp type 8
4        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
5        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
6        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpts:1:65535
7        0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpts:1:65535
8        0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 8
9        0     0 DROP       icmp --  eth0   *       0.0.0.0/0            0.0.0.0/0           icmp type 8

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 547 packets, 57096 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      666 69520 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
2        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1:65535
3        0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spts:1:65535
msfadmin@metasploitable:~$ sudo iptables -L INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere
```

Fuente: El autor

Para garantizar la efectividad del filtrado de paquetes, se ejecuta una prueba de escaneo de puertos por medio del comando ***nmap –Sv 192.168.0.3***. En la Figura 87 se refleja claramente que solo los puertos 80 (HTTP) y 21 (SSH) están abiertos, el puerto 443 (HTTPS) está cerrado porque no existe ningún aplicativo en ejecución que lo utilice y resto de puertos no permiten el acceso porque están siendo filtrados por IPTables.

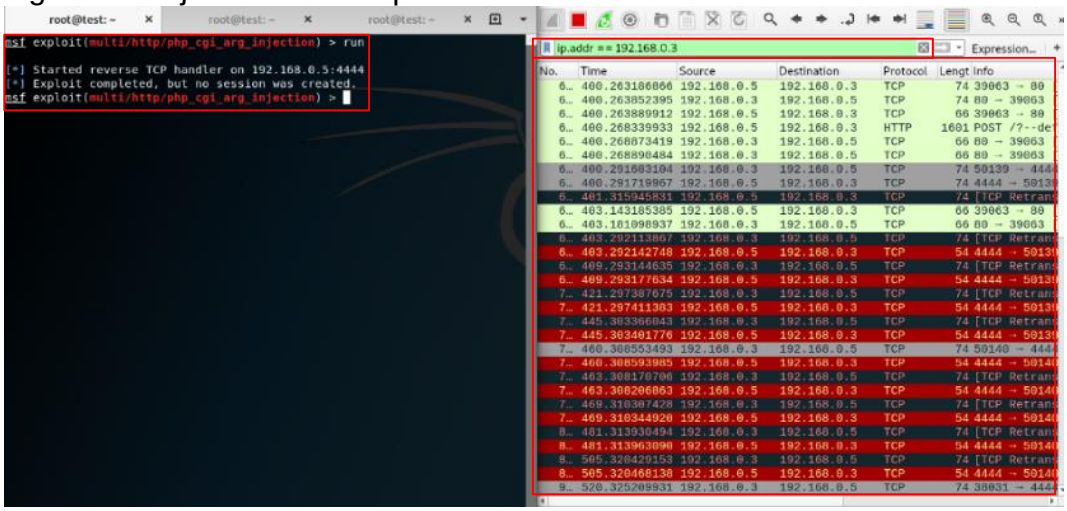
Figura 87. Escaneo de puertos escenario 1 sin resultado satisfactorio



Fuente: El autor

En la Figura 88 se observa que al ejecutar el exploit ***php_cgi_arg_injection***, no se establece la sesión, es decir, la conexión reversa TCP jamás se efectúa porque los puertos utilizados por Metasploit han sido bloqueados por las reglas de IPTables, además, también se observa retransmisión de paquetes sin respuesta y *reset* de la conexión de parte del servidor.

Figura 88. Ejecución del exploit escenario 1 sin resultado satisfactorio

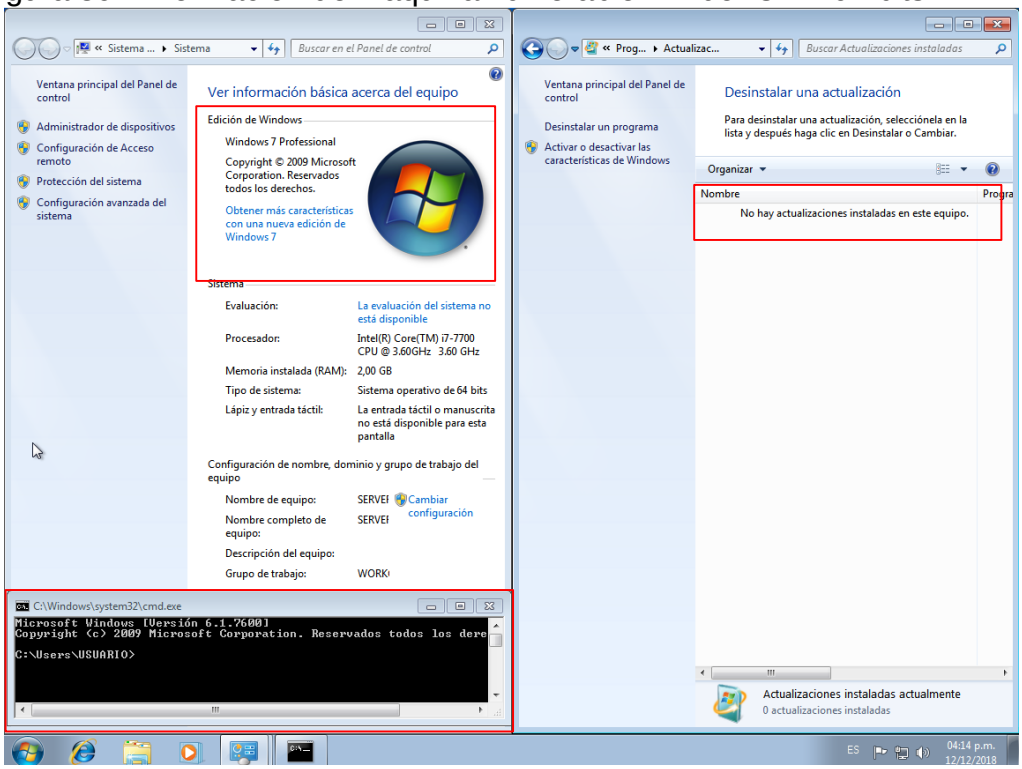


Fuente: El autor

6.2.2.8 Simulación del ataque 2 – *Eternalblue*. Continuando con el desarrollo del enfoque técnico; se presenta el escenario 2 donde se plantea la simulación del ataque *Eternalblue*, aprovechando una vulnerabilidad SMB (*Server Message Block*) - MS017-010 del lado del servidor con sistema operativo Windows 7.

- **Maquina Windows 7 vulnerable y desactualizada**. Desde VirtualBox se realiza la instalación de una máquina virtual con sistema operativo Windows 7 Enterprise a 64 bits, versión 6.1.7600; esta máquina no cuenta con ningún tipo de actualización o parche se seguridad instalado. En la Figura 89 se evidencian las características del sistema operativo simulado.

Figura 89. Información de maquina vulnerable Windows 7 X64 bits



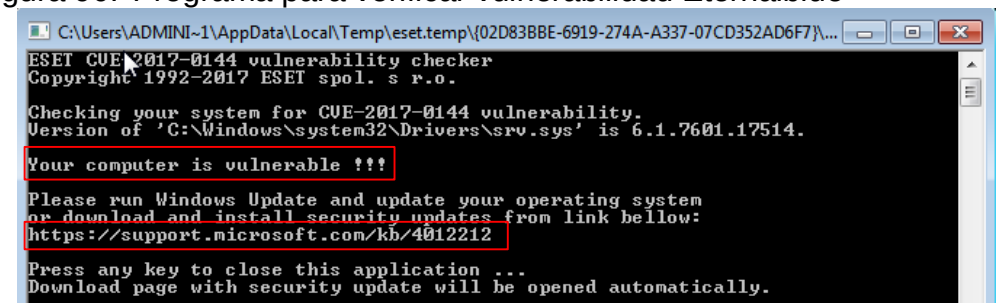
Fuente: El autor

Es necesario validar si la maquina Windows 7 es vulnerable al ataque *Eternalblue*; para esto se utiliza una herramienta de verificación del CVE 2017-0144, desarrollada por la reconocida empresa de seguridad ESET[64]. Se descarga el archivo ejecutable y se abre directamente una consola de

[64] ESET Latinoamérica, Verifica si tu PC está parcheada contra EternalBlue, el exploit de WannaCryptor, [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2017/05/16/check-eternalblue-pc-parcheada-wannacry/

comandos mostrando si el sistema operativo está expuesto a la vulnerabilidad del protocolo SMB. En la Figura 90 se evidencia que la máquina de pruebas es vulnerable al CVE 2017-0144.

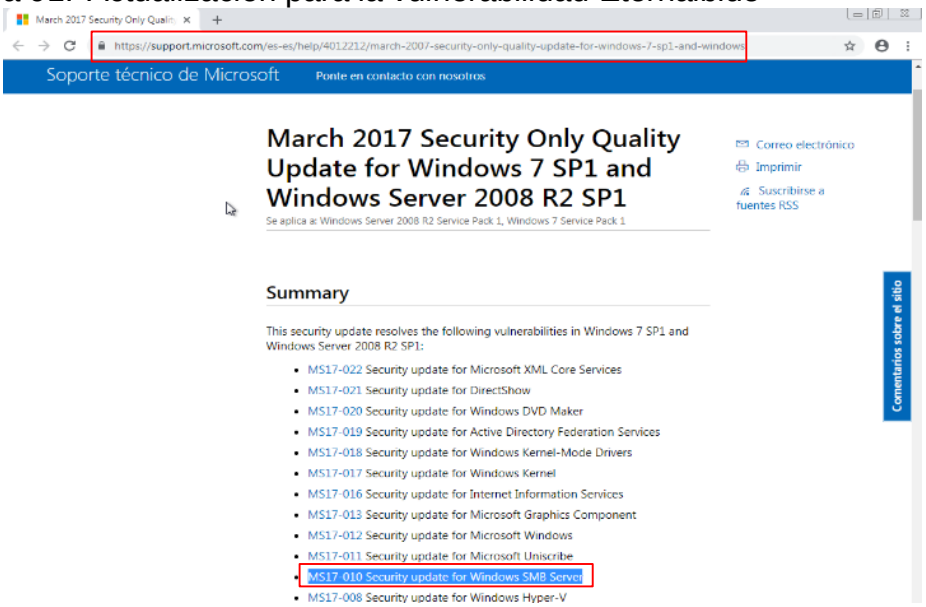
Figura 90. Programa para verificar vulnerabilidad Eternalblue



Fuente: El autor

Al digitar cualquier tecla, el programa abre el navegador web en la página de soporte técnico de Microsoft para descargar la actualización directamente desde el portal del fabricante. En la Figura 91 se muestra la elección de la actualización MS17_010 Actualización de seguridad para Windows SMB Server del mes de marzo, 2017.

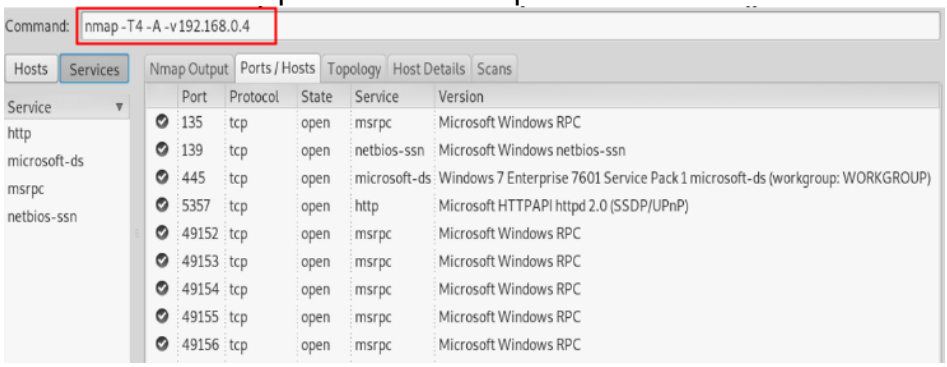
Figura 91. Actualización para la vulnerabilidad Eternalblue



Fuente: El autor

- **Análisis de NMAP escenario 2.** Se recopila información para llevar a cabo la explotación de vulnerabilidades e identificar algún tipo de control de seguridad. En la Figura 92 se visualiza la ejecución del comando ***nmap –T4 –A -v 192.168.0.4***, la salida evidencia las versiones de los puertos abiertos y que no existe ningún firewall de por medio.

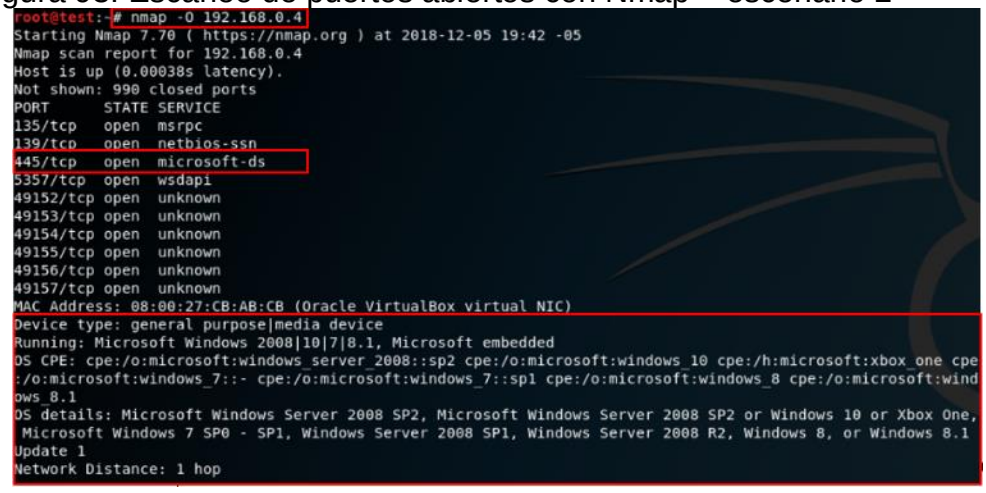
Figura 92. Escaneo de puertos filtrados por un firewall



Fuente: El autor

Continuando con el reconocimiento de la máquina vulnerable, es necesario identificar los puertos abiertos y el tipo de sistema operativo. En la Figura 93 se evidencia la ejecución del comando ***nmap –O 192.168.0.4***; esto permite identificar que el puerto TCP 445 se encuentra abierto y el sistema operativo de la maquina víctima es Microsoft Windows.

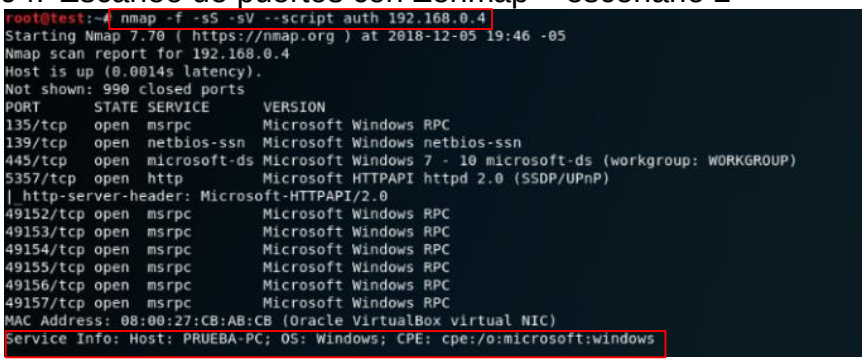
Figura 93. Escaneo de puertos abiertos con Nmap – escenario 2



Fuente: El autor

Desde una consola de comandos se digita ***nmap -f -sS -sV --script auth 192.168.0.4***, este script realiza un escaneo para validar la autenticación en los servicios disponibles. En la Figura 94 se observa el nombre de la maquina Windows, PRUEBA-PC, resultado de este comando.

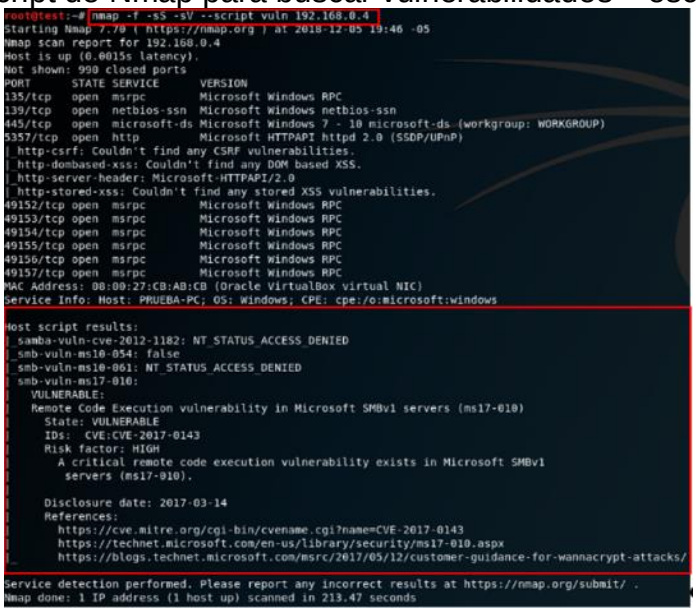
Figura 94. Escaneo de puertos con Zenmap – escenario 2



Fuente: El autor

Para ejecutar el script de búsqueda de vulnerabilidades se digita el comando ***nmap -f -sS -sV --script vuln 192.168.0.4.*** En la Figura 95 se detalla el listado de vulnerabilidades halladas en la maquina Windows 7.

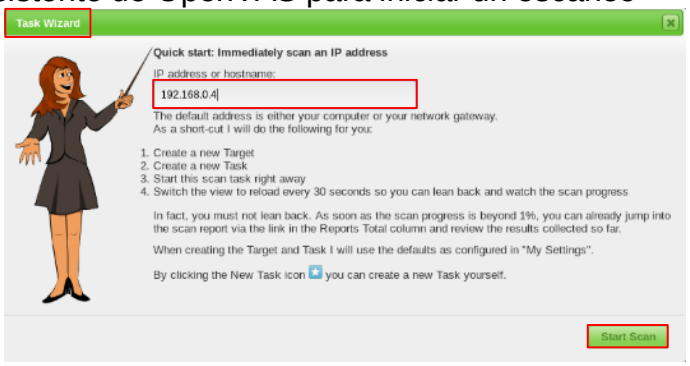
Figura 95. Script de Nmap para buscar vulnerabilidades – escenario 2



Fuente: El autor

• **Análisis de OpenVAS escenario 2.** Para ejecutar el escaneo de vulnerabilidades sobre la maquina vulnerable, se debe ir a la parte superior derecha en la opción ***Scans >> Task >> Task Wizard***, en el campo de texto se ingresa la dirección IP 192.168.0.4 y oprimir el botón ***Start Scan***, en la Figura 96 se observa el asistente de OpenVAS.

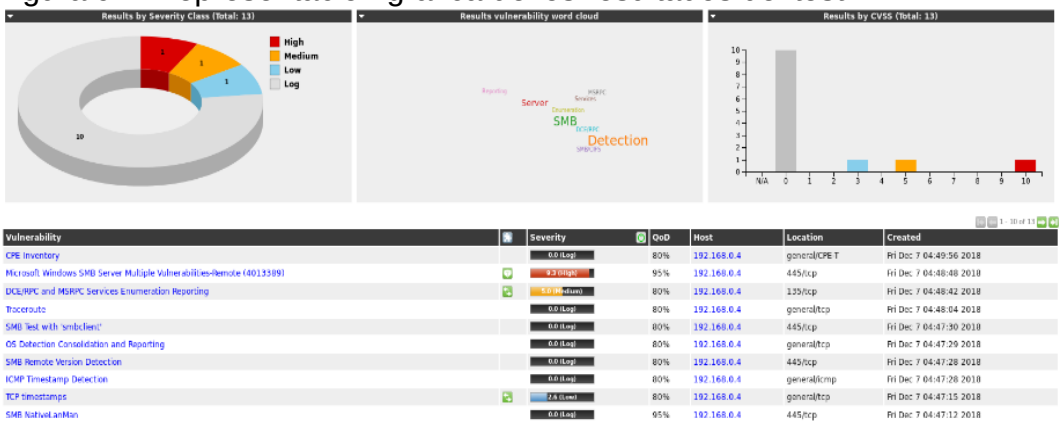
Figura 96. Asistente de OpenVAS para iniciar un escaneo



Fuente: El autor

Para el caso del escenario 2 se encontró 1 vulnerabilidad crítica, 1 con nivel medio, 1 con nivel baja y 10 archivos de logs analizados. En la Figura 97 se evidencia el resultado del escaneo sobre el servidor de la sede de Cali y las vulnerabilidades detectadas dependiendo su criticidad.

Figura 97. Representación gráfica de los resultados del test



Fuente: El autor

En la Figura 98 se observan las vulnerabilidades a nivel de aplicaciones y sus correspondientes puertos como MS Windows SMB, DCE/RPC & MSRPC, RCP *timestamps* entre otros. Es de resaltar que todas esas

aplicaciones son obsoletas, están desactualizadas y la mayoría representa un grado se severidad medio - alto.

Figura 98. Listado de vulnerabilidades por aplicación

Vulnerability	Severity	QoD	Host	Location	Created
CPE Inventory	0.0 (Log)	80%	192.168.0.4	general/CPE-T	Fri Dec 7 04:49:56 2018
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.0.4	445/tcp	Fri Dec 7 04:48:48 2018
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.4	135/tcp	Fri Dec 7 04:48:42 2018
Traceroute	0.0 (Log)	80%	192.168.0.4	general/tcp	Fri Dec 7 04:48:04 2018
SMB Test with 'smbclient'	0.0 (Log)	80%	192.168.0.4	445/tcp	Fri Dec 7 04:47:30 2018
OS Detection Consolidation and Reporting	0.0 (Log)	80%	192.168.0.4	general/tcp	Fri Dec 7 04:47:29 2018
SMB Remote Version Detection	0.0 (Log)	80%	192.168.0.4	445/tcp	Fri Dec 7 04:47:28 2018
ICMP Timestamp Detection	0.0 (Log)	80%	192.168.0.4	general/icmp	Fri Dec 7 04:47:28 2018
TCP timestamps	2.6 (Low)	80%	192.168.0.4	general/tcp	Fri Dec 7 04:47:15 2018
SMB NativeLanMan	0.0 (Log)	95%	192.168.0.4	445/tcp	Fri Dec 7 04:47:12 2018
DCE/RPC and MSRPC Services Enumeration	0.0 (Log)	80%	192.168.0.4	135/tcp	Fri Dec 7 04:47:28 2018
SMB/CIFS Server Detection	0.0 (Log)	80%	192.168.0.4	445/tcp	Fri Dec 7 04:47:28 2018
SMB/CIFS Server Detection	0.0 (Log)	80%	192.168.0.4	139/tcp	Fri Dec 7 04:47:15 2018

Fuente: El autor

En la Figura 99 se muestra la ficha técnica de la vulnerabilidad ***CVE-2017-0143 MS Windows SMB Server Multiple Vulnerabilities Remote***, esto indica un fallo de seguridad del protocolo SMB que le permite a un atacante ejecutar código remotamente en sistemas operativos Windows.

Figura 99. Información de OpenVAS sobre una vulnerabilidad

Result: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) Modified: Fri Dec 7 04:48:48 2018 Owner: root

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.0.4	445/tcp	

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)
Version used: $Revision: 11874 $

References
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
BID: 96703, 96704, 96705, 96707, 96709, 96706
CERT: CB-K17/0435, DFN-CERT-2017-0448
Other: https://support.microsoft.com/en-in/kb/4013078

Fuente: El autor

En el Cuadro 6 se encuentra registrada la descripción de las vulnerabilidades con mayor nivel de riesgo para el servidor de la sede Cali, según el CVSS (*Common Vulnerability Score System*).

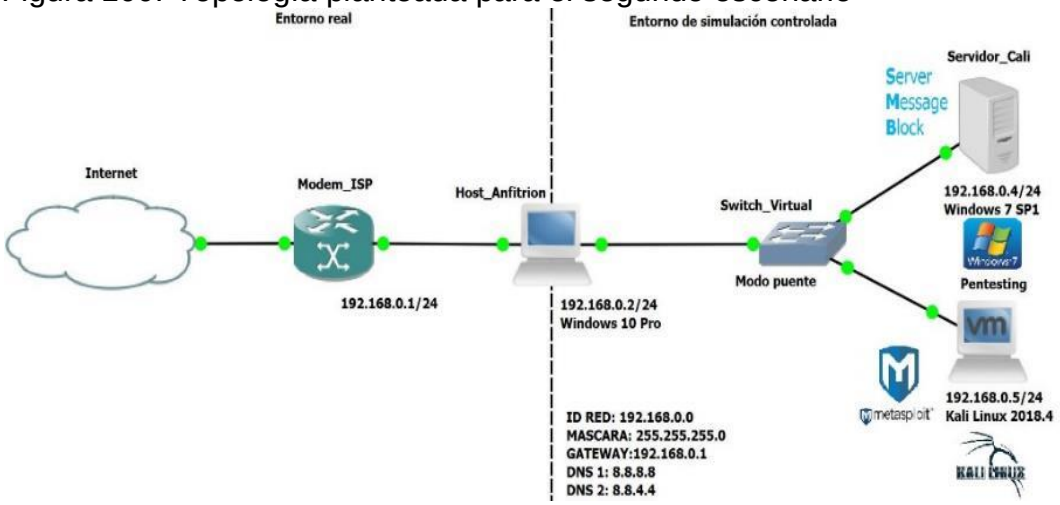
Cuadro 6.Top de vulnerabilidades encontradas en el servidor de Cali

Código CVE	Descripción	CVSS	Producto afectado
CVE-2006-3439	Desbordamiento de buffer en entornos Windows le permite a usuarios anónimos y atacantes la ejecución de código remoto por medio de un RPC.	10	Microsoft Windows
CVE-2009-2532	Ejecución de código remoto basado en una vulnerabilidad del protocolo SMB v2 que no maneja la negociación del protocolo SMB.	10	Microsoft Windows
CVE-2009-3103	Error en la implementación del protocolo SMBv2, provocando una denegación de servicio o ejecución de código remoto.	10	Microsoft Windows
CVE-2017-0143	Permite la ejecución de código remoto aprovechando una vulnerabilidad en el protocolo SMB.	9.3	Microsoft Windows
CVE-2017-0144	Permite la ejecución de código remoto aprovechando una vulnerabilidad en el protocolo SMB.	9.3	Microsoft Windows
CVE-2017-0145	Permite la ejecución de código remoto aprovechando una vulnerabilidad en el protocolo SMB.	9.3	Microsoft Windows
CVE-2017-0146	Permite la ejecución de código remoto aprovechando una vulnerabilidad en el protocolo SMB.	9.3	Microsoft Windows
CVE-2017-0147	Permite obtener datos de la memoria RAM aprovechando una vulnerabilidad en el protocolo SMB.	9.3	Microsoft Windows
CVE-2017-0148	Permite la ejecución de código remoto aprovechando una vulnerabilidad en el protocolo SMB.	9.3	Microsoft Windows
Fuente: El autor, basado en Common Vulnerabilities and Exposures.			

- **Ataque Eternalblue con Metasploit.** Con base en la información recolectada previamente, se ha identificado una vulnerabilidad sobre el protocolo SMB (*Server Message Block*) que permite ejecutar código remotamente en diferentes versiones de Microsoft Windows. Tal vulnerabilidad está relacionada con el código CVE-2017-0143: *Eternalblue,* este *exploit* aprovecha un fallo en la versión 1 del protocolo SMB para enviar paquetes específicos que permiten la ejecución de código remotamente en una host víctima.

En la Figura 100 se muestra la topología para el desarrollo de este escenario es un ambiente controlado de red de área local (LAN) por medio de un conmutador virtual y sin firewall de por medio.

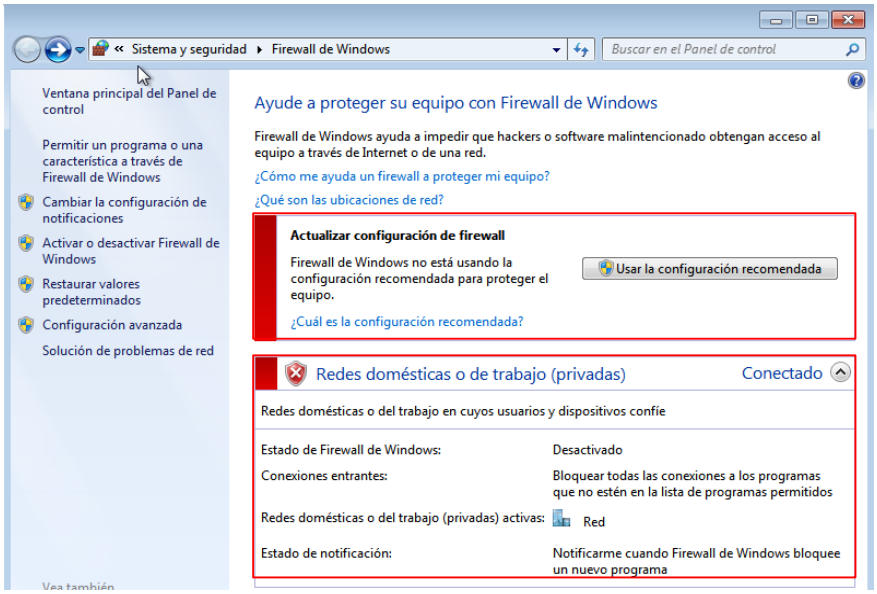
Figura 100. Topología planteada para el segundo escenario



Fuente: El autor

Antes de iniciar la explotación de la vulnerabilidad sobre el protocolo SMB en la maquina Windows 7, es necesario validar que el firewall de Windows este deshabilitado. Se debe ingresar a la ruta ***Panel de control\Sistema y seguridad\Firewall de Windows*** y deshabilitarlo temporalmente. En la Figura 101 se aprecia que el firewall de Windows se encuentra inactivo.

Figura 101. Firewall de Windows deshabilitado



Fuente: El autor

Es necesario verificar si existen *exploits* para ejecutar el ataque de tipo *EternalBlue*, por lo tanto, en la Figura 102 se ejecuta el comando ***search*** acompañado de un parámetro para realizar la búsqueda, en este caso se especificó ***ms17_010_eternalblue*** para que la consulta sea más eficiente.

Figura 102. Búsqueda del módulo EternalBlue para ejecutar el ataque

Fuente: El autor

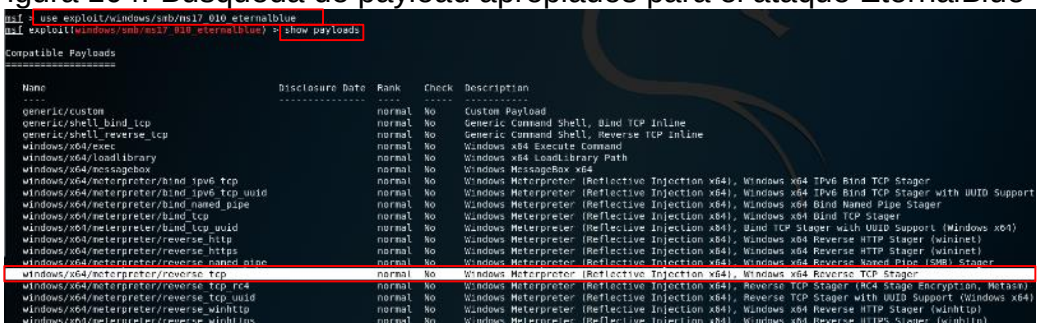
En la Figura 103 se aprecia la información detallada del exploit a través del comando ***info exploit/windows/smb_ms17_010_eternalblue.*** El *exploit* fue publicado el 14/03/2017 y se utiliza en versiones de Windows 7 y server 2008 R2 que son vulnerables al desbordamiento de buffer SMB Versión 1. En algunos sistemas puede generar inestabilidad y en ocasiones aparece pantalla azul con un error o reinicios no programados.

Figura 103. Información detallada del exploit smb_ms17_010_eternalblue

Fuente: El autor

En la Figura 104 se visualiza el comando ***use exploit/windows/smb_ms17_010_eternalblue*** para seleccionar el exploit adecuado, después se usa la opción ***show payloads*** para elegir la carga útil de la conexión TCP reversa, ***windows/x64/meterpreter/reverse_tcp.*** Este ataque compromete la maquina afectada permitiendo obtener acceso remoto a la webcam y captura de las pulsaciones del teclado

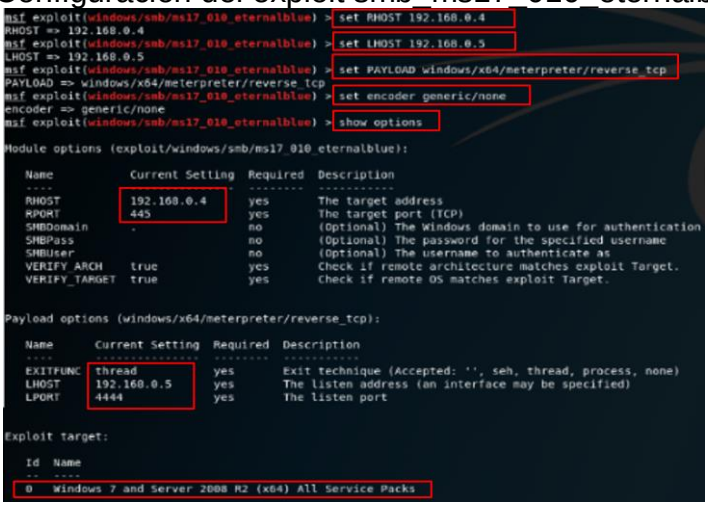
Figura 104. Búsqueda de payload apropiados para el ataque EternalBlue



Fuente: El autor

En la Figura 105 se configura la herramienta Metasploit con la información del host remoto vulnerable (***RHOST***), host local que va a ejecutar el exploit (***LHOST***), payload seleccionado (***windows/x64/meterpreter/reverse_tcp***) y por último se muestra las opciones de la configuración del ataque usando el comando ***show options.***

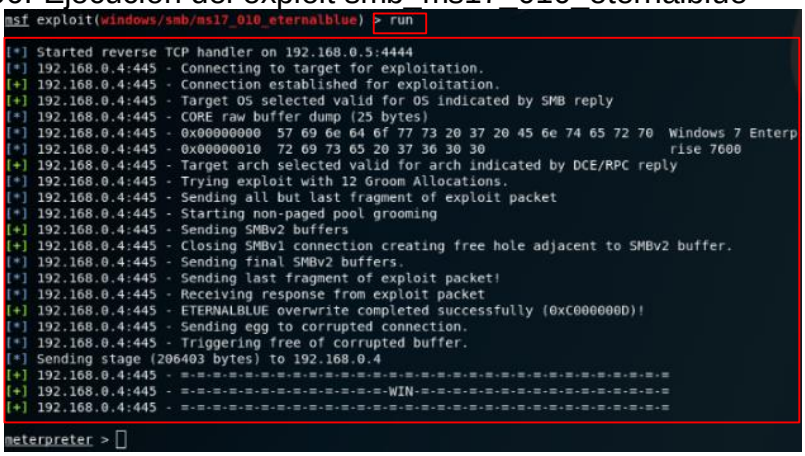
Figura 105. Configuración del exploit smb_ms17_010_eternalblue



Fuente: El autor

En la Figura 106 se presenta la ejecución automatizada del ataque por medio del comando ***run.*** En la consola se observa el progreso de la conexión TCP inversa y el establecimiento de ***Meterpreter***; este intérprete de comandos permite la ejecución remota de instrucciones e interacción con la víctima.

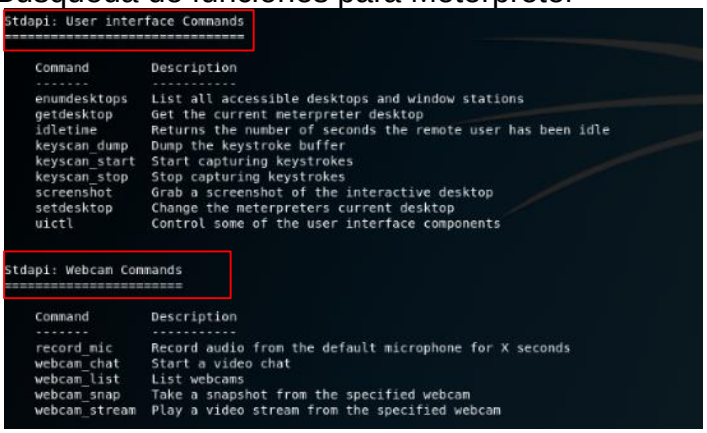
Figura 106. Ejecución del exploit smb_ms17_010_eternalblue



Fuente: El autor

Meterpreter ofrece diferentes funciones y herramientas para comprometer la maquina vulnerada, para conocer el conjunto de comandos se debe preguntar con el signo **?**, solo o acompañado de una palabra clave. En la Figura 107 se listan algunas de las herramientas de Meterpreter.

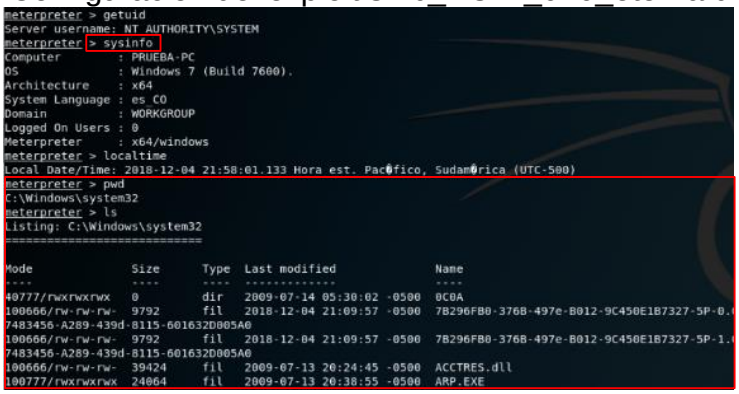
Figura 107. Búsqueda de funciones para Meterpreter



Fuente: El autor

Tras comprometer la máquina Windows 7 y establecer la sesión con *Meterpreter*, se usan comandos: ***sysinfo*** para conocer información del sistema, ***localtime*** para saber la configuración horaria, ***pwd*** para saber en qué directorio está situado y ***ls*** para listar el contenido del directorio actual. En la Figura 108 se evidencia control sobre la máquina, además de la ubicación actual y contenido del directorio ***C:\windows\system32***.

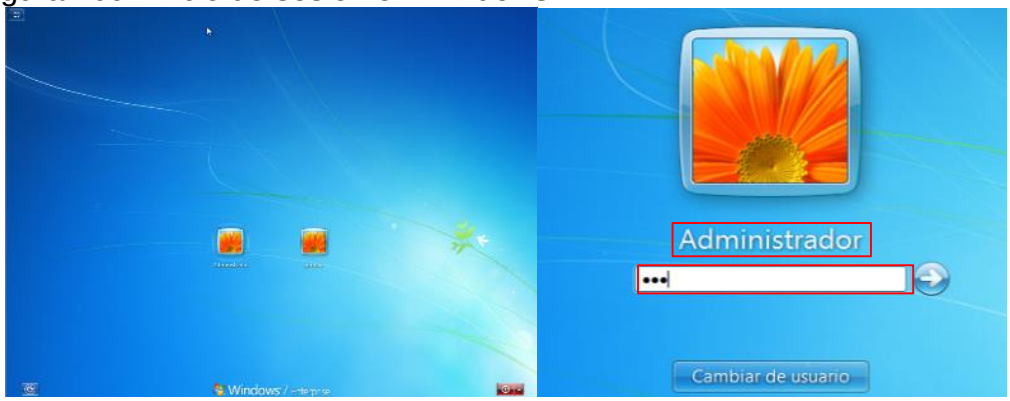
Figura 108. Configuración del exploit smb_ms17_010_eternalblue



Fuente: El autor

- **Keylogger y acceso a cámara web.** Inicialmente la maquina vulnerable con Windows 7 no ha iniciado sesión, esto con la finalidad de realizar la captura de la contraseña de un usuario, en la Figura 109 se observa que el usuario de ejemplo será el administrador del sistema.

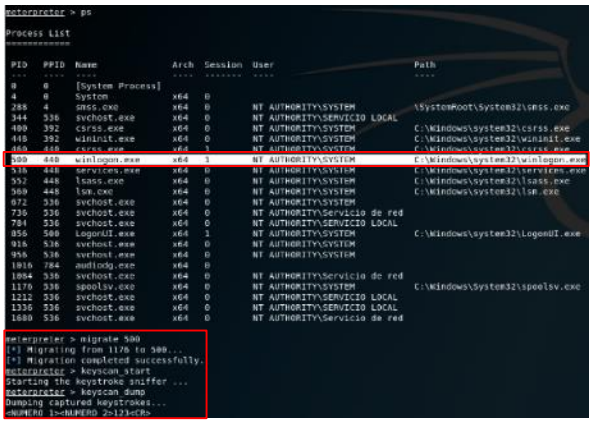
Figura 109. Inicio de sesión en Windows 7



Fuente: El autor

Se digita el comando ***ps*** para listar los procesos activos y se identifica el PID, (*Process Identificator*), de la aplicación ***winlogon.exe***, con este valor se procede a digitar el comando ***migrate 500***, para migrar el proceso de inicio de sesión al metainterprete. En la Figura 110 se observa la captura de pulsaciones usando el comando ***keyscan_start*** y para ver los caracteres capturados se digita el comando ***keyscan_dump***.

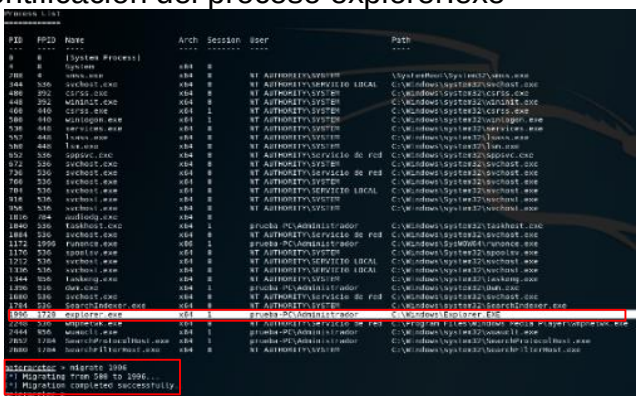
Figura 110. Captura de la contraseña de inicio de sesión



Fuente: El autor

Con la sesión habilitada, en la Figura 111 se identifica el PID del proceso ***explore.exe*** a través del comando ***ps*** que en esta ocasión es ***1996***, sin embargo, esto cambia dinámicamente con cada inicio de sesión. Este proceso del sistema será utilizado para la captura de pulsaciones en aplicaciones que se ejecutan en primer plano en el sistema operativo.

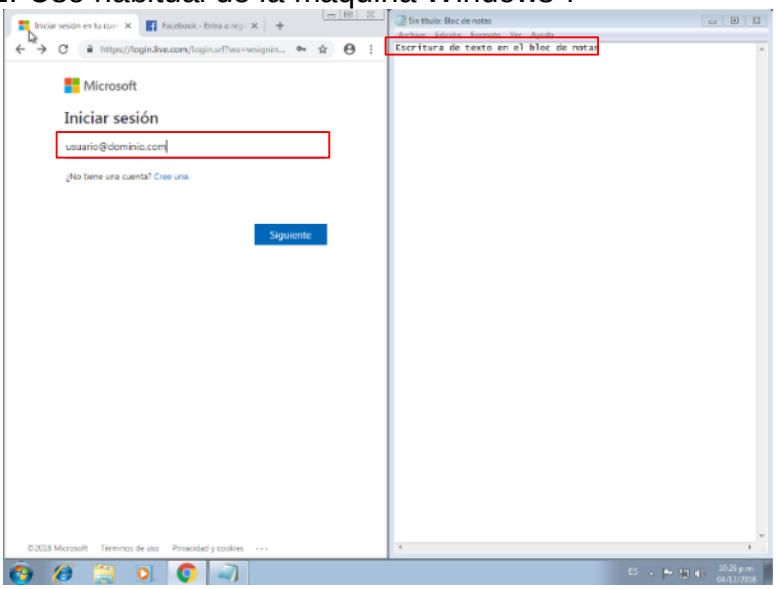
Figura 111. Identificación del proceso explorer.exe



Fuente: El autor

Con la configuración establecida para capturar las pulsaciones del teclado, en la Figura 112 se procede a usar habitualmente la maquina Windows 7 ingresando a un sitio web con usuario y contraseña, además también se ejecuta un bloc de notas para llevar apuntes e ingresar caracteres.

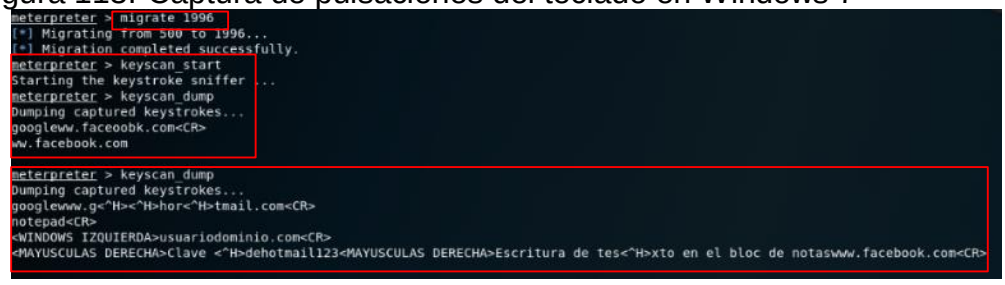
Figura 112. Uso habitual de la maquina Windows 7



Fuente: El autor

Se inicia la captura de pulsaciones usando el comando ***migrate 1996***, esto permite migrar el proceso del explorador de Windows al metainterprete, después se digita ***keyscan_start***, lo cual inicia la captura de pulsaciones. En la Figura 113 se pueden ver los caracteres capturados mediante el comando ***keyscan_dump***.

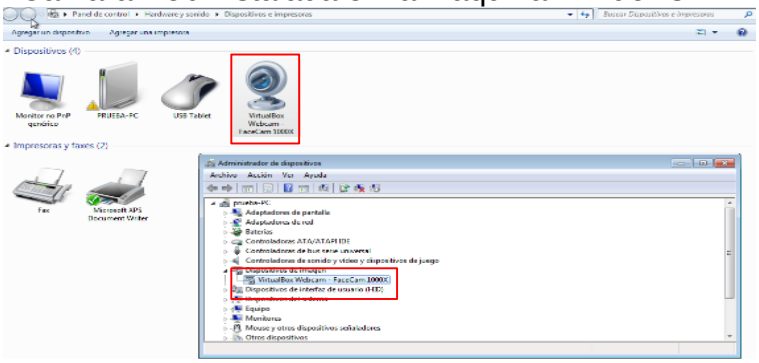
Figura 113. Captura de pulsaciones del teclado en Windows 7



Fuente: El autor

La máquina Windows 7 cuenta con una cámara web como periférico de entrada, el cual será comprometido de manera remota para capturar el video. En la Figura 114 se observa que la cámara web está en línea y se encuentra correctamente instalada en el sistema operativo.

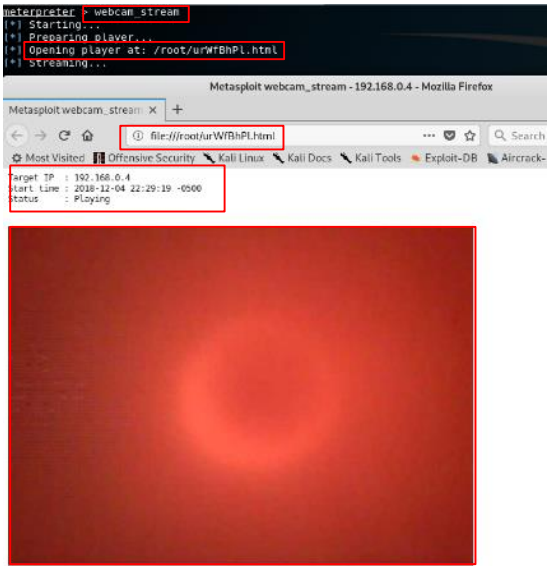
Figura 114. Cámara web instalada en la maquina Windows 7



Fuente: El autor

En la Figura 115 se observa el proceso para obtener el video de la cámara web se digita el comando ***webcam_stream*** y automáticamente se abre un navegador web donde se observa el video de la cámara web, fecha de captura y la dirección IP de la maquina comprometida.

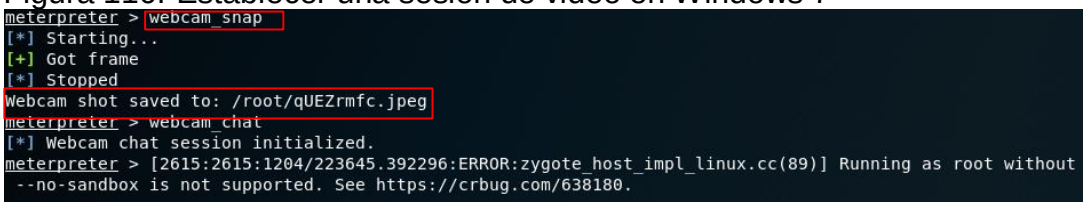
Figura 115. Captura de video de la cámara web en Windows 7



Fuente: El autor

En la Figura 116 se muestra la opción de captura de pantalla, *snapshot*, al video de la cámara web a través del comando ***webcam_snap***, esta imagen se almacena en la carpeta home de Kali Linux en formato .jpg. Existe la posibilidad de crear una sesión de videoconferencia remotamente a través del comando ***webcam_chat***.

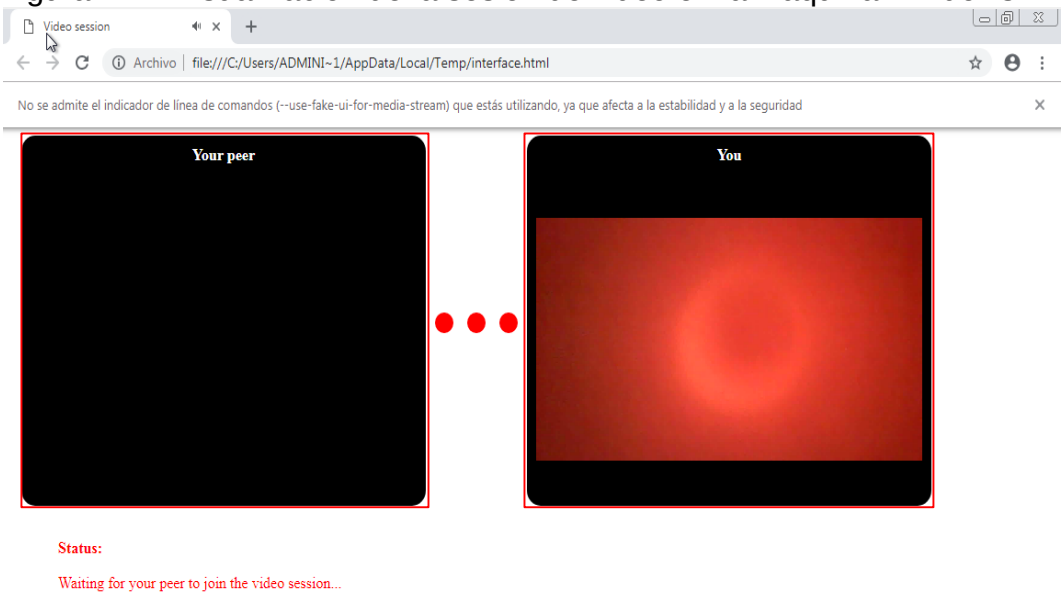
Figura 116. Establecer una sesión de video en Windows 7



Fuente: El autor

En la Figura 117 es claramente visible que después de realizar el ataque y comprometer la cámara web, del lado de la maquina Windows 7 vulnerable, se abre automáticamente un navegador web donde se observa el video de las cámaras de ambos equipos, además, también se tiene audio para establecer una conversación entre el atacante y la víctima.

Figura 117. Visualización de la sesión de video en la maquina Windows 7



Fuente: El autor

- **Políticas de seguridad.** La Empresa RANDOM S.A. se ha comprometido con la definición de lineamientos y disposiciones de alto nivel, que tienen como finalidad garantizar y proteger la confidencialidad, integridad y disponibilidad de la información propia, de clientes, de colaboradores y de terceros; la cual es requerida para la correcta operación del negocio en cumplimiento de su visión, misión y objetivos estratégicos.
La presente política aplica de manera transversal para todos los recursos tecnológicos de RANDOM S.A. y es de carácter obligatorio su cumplimiento de parte de todos los usuarios que tengan algún tipo de vínculo con los activos de la información.

- **Uso aceptable de los activos de información:** Cualquier activo de información de la empresa debe ser usado única y exclusivamente para propósitos laborales. Está prohibido la trasferencia de información desde y/o hacia fuentes externas con procedencia desconocida, además, se sanciona la difusión de malware o cualquier otro tipo de código malicioso que afecte la infraestructura tecnológica. Se restringe el acceso a páginas que agredan la ética y el buen comportamiento, así como la visualización de páginas de contenido explicito, ofensivo, injurioso, obsceno, y/o que atenten contra la integridad moral de las personas o de la organización.

  Los activos de la información asignados por la organización se deben emplear para el correcto desarrollo de las funciones del cargo y bajo la responsabilidad del colaborador al cual le fueron asignados, por lo tanto, no pueden se pueden utilizar con fines personales o por terceros no autorizados.

- **Revisión de permisos de acceso:** Los permisos y privilegios de acceso a los sistemas informáticos de la organización deben ser revisados semestralmente o después de cualquier cambio significativo. Los accesos a los sistemas informáticos de la organización deben estar controlados por autenticación de doble factor, siempre y cuando la tecnología lo permita. Las contraseñas deben cumplir con parámetros de longitud y combinación de caracteres alfanuméricos y el cambio de la contraseña se debe realizar a intervalos regulares 30 días.

- **Manejo del correo electrónico:** El correo electrónico debe ser usado únicamente para el envío y recepción de mensajes electrónicos relacionados con la organización. Por ende, se prohíbe el uso con fines personales, económicos, comerciales o cualquier otro uso ajeno a la organización. Cualquier mensaje SPAM, difusión de mensajes en cadena y remitente sospechoso, debe ser informando al Oficial de seguridad, privacidad y cumplimiento y posteriormente eliminado, debido a que

puede tener adjunto algún tipo de malware o tener en su contenido elementos de difamación o suplantación.

- **Clasificación y manejo de la información:** Todo usuario de RANDOM S.A. deberá tener asignado una cuenta de dominio y una contraseña, de acuerdo a los estándares establecidos por la Oficina de Sistemas. El uso de la misma es responsabilidad de la persona a la que le fue asignada, ya que su uso es carácter personal e intransferible. La información de uso interno es responsabilidad del dueño o usuario final y en general por todas las áreas que legítimamente deben tener acceso a ella.

  Es obligación de cada responsable de la información, clasificarla bajo los criterios definidos. Teniendo en cuenta su clasificación, la información Confidencial debe ser etiquetada como tal de una forma visible, de acuerdo a lo establecido en el procedimiento de clasificación y etiquetado de activos de información. El acceso a la información confidencial debe ser controlado independientemente del estado en que se encuentre, física o digital.

- **Seguridad en los procesos:** velar por el correcto funcionamiento y la seguridad de infraestructura tecnológica, para esto se debe establecer los roles, responsabilidades, técnicas y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información. Se debe implementar la segregación de funciones, cuando aplique, a fin de reducir el riesgo del uso negligente o mal uso deliberado de los sistemas. Es responsabilidad de cada funcionario de RANDOM S.A. cerrar las sesiones de trabajo abiertas en los diferentes sistemas de información, correo electrónico y demás aplicaciones de la entidad al finalizar la jornada de trabajo.

- **Seguridad física:** Se debe contar con mecanismos de control de acceso tales como puertas de seguridad, torniquetes, sistemas de control con tarjetas de proximidad, sistemas biométricos, sistema de alarmas, sistemas de control de incendios y circuitos cerrados de televisión en las áreas que sean consideradas de alta criticidad para la entidad.

  Para el ingreso al centro de cómputo y otras zonas catalogadas como críticas, el personal encargado de actividades de instalación, remoción y/o mantenimiento de hardware y software, mantenimiento de los sistemas de control y personal de limpieza deberán estar identificados plenamente en sus actividades y estarán acompañados permanentemente por el personal de la Oficina de Sistemas.

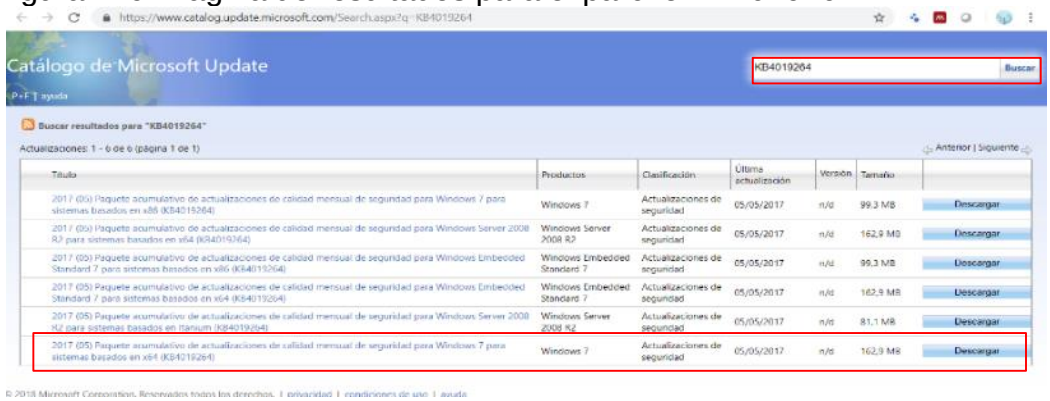
- **Instalación de la actualización MS17-010.** Como parte del proceso de prevención para evitar que una maquina con sistema operativo Windows sea comprometida por un ataque *Eternalblue*, Microsoft ha dispuesto las actualizaciones KB4012212 y KB4019264 que eliminan este fallo de seguridad. Estos parches se encuentran disponibles en las actualizaciones automáticas del sistema o pueden ser instaladas manualmente desde el catálogo de Microsoft *Update, e*n la Figura 118 se muestra la URL https://www.catalog.update.microsoft.com.

Figura 118. Página principal del catálogo de Microsoft Update

Fuente: El autor

En la Figura 119 se muestra el proceso de búsqueda de la actualización MS17-010, para este caso se realizará el proceso con el parche de seguridad KB4019264 para Windows 7 de 64 bits.

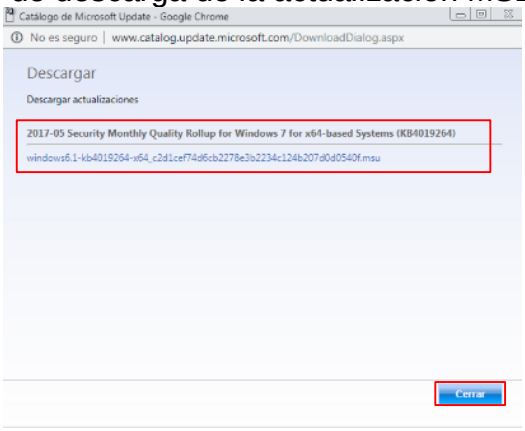
Figura 119. Página de resultados para el parche KB4019264



Fuente: El autor

Se elige la actualización correcta para el sistema operativo y al oprimir el botón descargar, aparece una ventana emergente donde se visualiza el enlace de descarga del archivo de actualización, en la Figura 120 se observa que la descarga seleccionada es el parche de seguridad KB4019264.

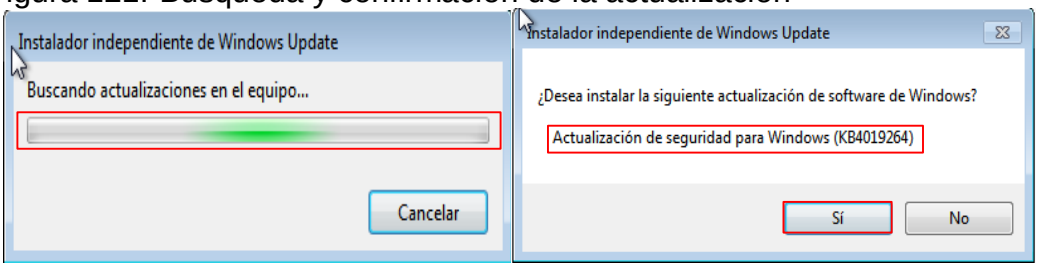
Figura 120. Enlace de descarga de la actualización MS17-010



Fuente: El autor

Al finalizar la descarga, se procede a ejecutar el archivo msu, (*Windows Update Standalone Installer*), con permisos de administrador. En la Figura 121 se visualiza la ventana en búsqueda de la actualización para validar si está instalada, después se debe confirmar que se desea realizar la instalación del parche de seguridad KB4019264.

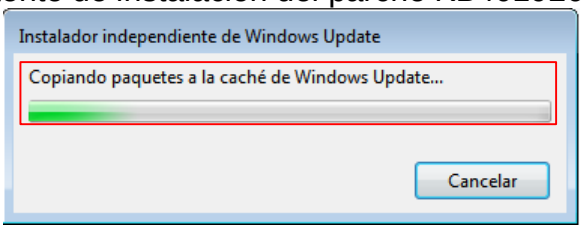
Figura 121. Búsqueda y confirmación de la actualización



Fuente: El autor

En la Figura 122 se aprecia que el proceso de instalación inicia copiando los paquetes en la partición local C, por ende, se debe contar con mínimo 2 GB de almacenamiento disponibles, después el asistente se encarga de la instalación de la actualización KB4019264.

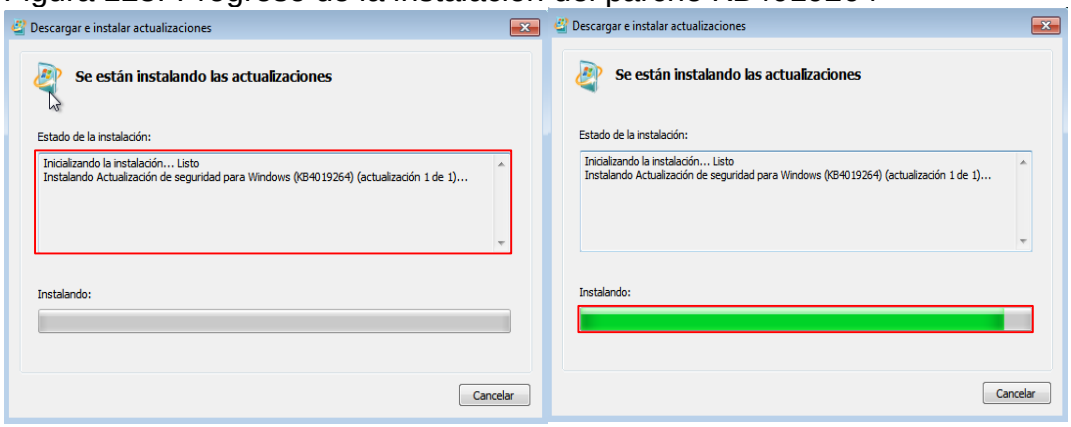
Figura 122. Asistente de instalación del parche KB4019264



Fuente: El autor

El asistente se ejecuta en primer plano, en la Figura 123 se observa el proceso de la instalación, el cual tarda un tiempo considerable porque deben ser descargados todos los paquetes y posteriormente instalados sobre el sistema operativo.

Figura 123. Progreso de la instalación del parche KB4019264

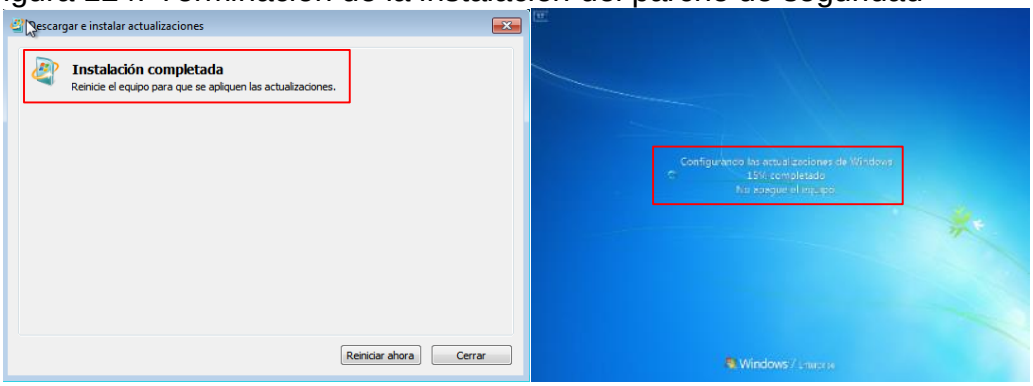


Fuente: El autor

En este punto es importante aclarar que la actualización KB4019264 fue liberada por Microsoft[65] el 9 de mayo de 2017 y es un paquete acumulativo de seguridad que corrige algunos errores identificadas en actualizaciones anteriores, reemplazando a la actualización KB4012212. En la Figura 124 se aprecia la culminación del proceso de instalación con un reinicio del sistema que permite configurar la actualización y que los cambios sean aplicados, este puede tardar varios minutos dependiendo de los recursos físicos asignados a la máquina.

[65] SOPORTE TÉCNICO DE WINDOWS, 9 de mayo de 2017: KB4019264 (paquete acumulativo mensual), [En línea]. Disponible en: <https://support.microsoft.com/es-co/help/4019264/windows-7-update-kb4019264>.

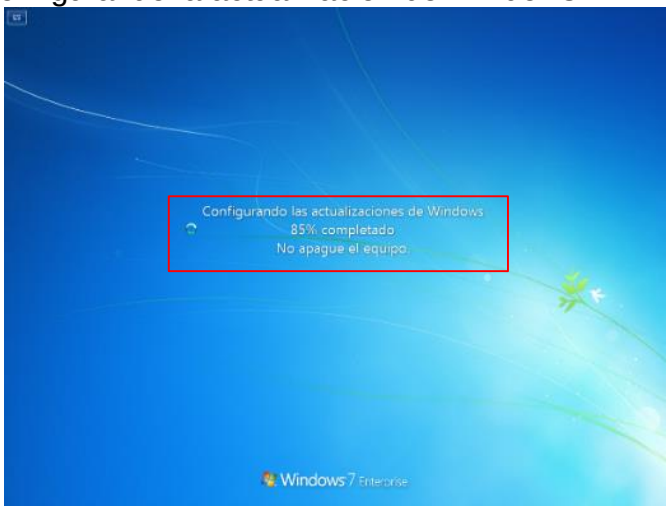
Figura 124. Terminación de la instalación del parche de seguridad



Fuente: El autor

En la Figura 125 se observa que después del reinicio, el sistema continúa ejecutando los últimos ajustes de la actualización KB4019264, por lo tanto, se recomienda no apagar el equipo hasta que se apliquen todos los ajustes del parche de seguridad y el sistema operativo esté listo para funcionar.

Figura 125. Configurando la actualización de Windows 7

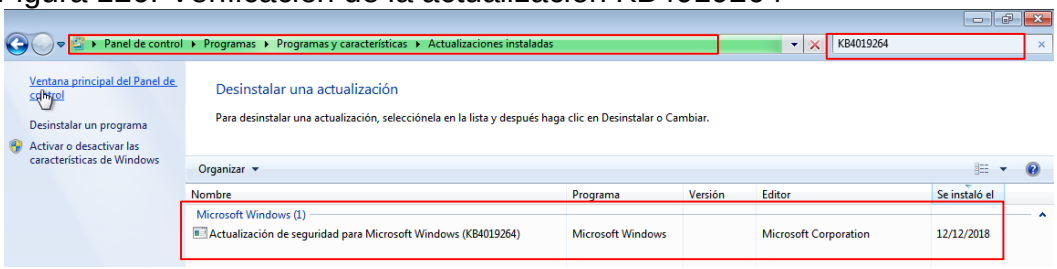


Fuente: El autor

Una vez se ha instalado el parche de seguridad KB4019264, es pertinente comprobar que la actualización este instalada en el sistema y que cumpla su función; proteger al sistema de ataques tipo *Eternalblue*. En la Figura 126 se observa una ventana del panel de control, en la sección de programas y características se elige la opción de actualizaciones instaladas. En esta ventana aparece un campo de texto ubicado en la parte superior derecha,

donde se digita el nombre de la actualización KB4019264 y en la parte inferior se observa que la misma ha sido instalada correctamente.

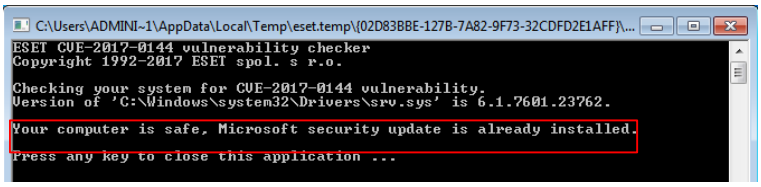
Figura 126. Verificación de la actualización KB4019264



Fuente: El autor

En la Figura 127 se observa que al ejecutar nuevamente el utilitario de ESET; esta vez muestra que el sistema está a salvo y que la actualización está instalada correctamente, esto quiere decir que el sistema no es vulnerable.

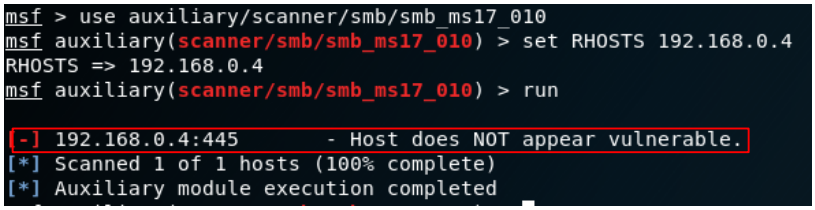
Figura 127. Verificación de la actualización KB4019264



Fuente: El autor

En la Figura 128 se aprecia que al ejecutar el exploit para la vulnerabilidad MS17_010, el sistema operativo ya no es susceptible ante este tipo de ataques.

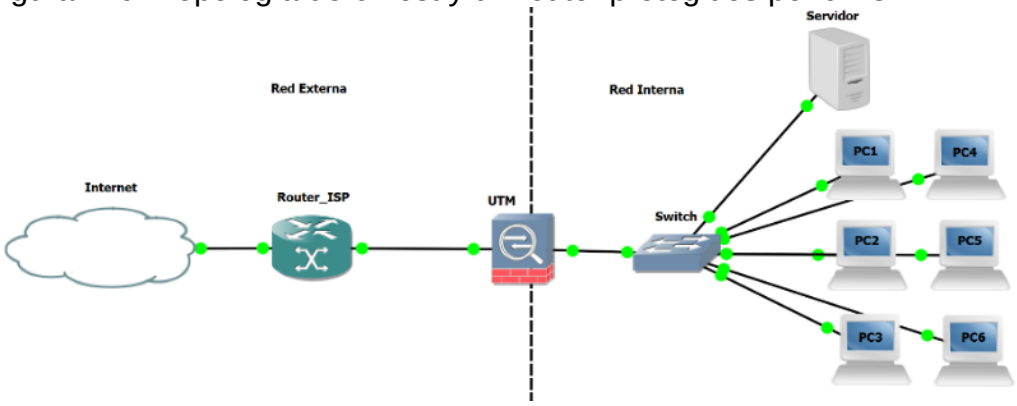
Figura 128. Verificación de la actualización KB4019264 desde Metasploit



Fuente: El autor

- **Mejorar en la seguridad de la organización.** La sede de Cali tiene pocos activos de la información, por lo tanto, es pertinente realizar una propuesta acorde con la demanda de tráfico y cantidad de usuarios. Para esto se propone la implementación de un dispositivo UTM que ofrezca gestión unificada de la seguridad en la red interna, además se recomienda tener internamente un servidor antivirus con una solución de antivirus de tal manera que la seguridad se establezca de manera perimetral e internamente. En la Figura 129 se presenta la propuesta de topología para la red interna de la sede de Cali.

Figura 129. Topología de 6 host y un router protegidos por un UTM



Fuente: El autor

- **UTM (Unified Threat Management):** Gestión Unificada de Amenazas, es una solución de seguridad integral en un solo dispositivo que posee diferentes funcionalidades. Un UTM se destaca por sus múltiples características de seguridad, sencillez, simplificación de la infraestructura de red, fácil administración y reducción de gastos. A nivel funcional un UTM está capacitado para realizar las siguientes acciones:

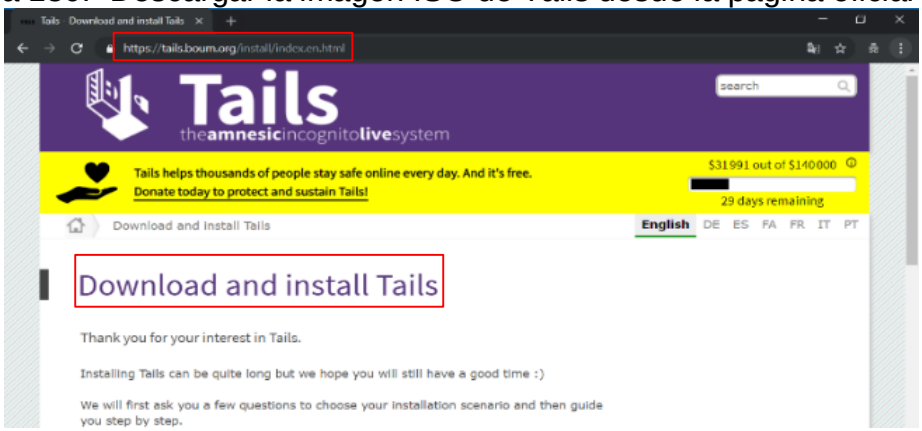
  - Módulos de antivirus, antispyware y *antispam*.
  - Firewall para el filtrado de paquetes.
  - Inspección profunda basado en SSL.
  - Sistemas de detección y prevención de intrusos
  - Análisis de tráfico basado en contenido web y control de aplicaciones.
  - Enrutamiento estático y dinámico.
  - Traducción de direcciones de red NAT (*Network Address Translation*). y re-direccionamiento de puertos PAT (*Port Address Translation*).
  - VPN (SSL y IPSec), canal cifrado de comunicaciones.
  - Compatibilidad con tecnologías emergentes como Cloud Computing, SDN (*Software Defined Network*) e IPv6.

Este tipo de solución presenta algunas desventajas, cómo, por ejemplo, un punto único de falla o agotamiento de recursos que al tener muchas funcionalidades incluidas genera desbordamiento de la capacidad del dispositivo. La recomendación inicial es hacer un estudio previo para contrastar la demanda de la red con las características del equipo UTM y elegir el dispositivo más apropiado, otra recomendación útil es solventar el punto único de falla con alta disponibilidad a nivel del UTM e incluir otro tipo de medidas de seguridad perimetral basadas en software.

- **Servidor Endpoint**: Está diseñado para detectar, prevenir, eliminar y controlar la presencia de software malicioso y otras vulnerabilidades en los sistemas, host, servicios y archivos que llegan desde internet, también los remitidos en medios extraíbles. La solución *Endpoint* considera el servicio de NIDS (Sistema de Detección de Intrusos basado en Red), para la detección de intrusos a nivel de *host*, con la finalidad de prevenir y alertar las anomalías a nivel de host. Los cuales para el caso presentado se encuentra vulnerables debido a que los *hosts* están expuestos sin los controles suficientes hacia Internet y correspondientes actualizaciones de seguridad.

- **Ingreso a la Deep Web.** Para ingresar al Internet no visible se utilizará TAILS (*The Amnesic Incognito Live System*). En la Figura 130 se muestra el repositorio oficial de TAILS[66], en este sitio es posible descargar el archivo .iso que contiene la imagen pre configurada del sistema operativo TAILS, al finalizar la descarga se debe guardar el archivo localmente.

Figura 130. Descargar la imagen ISO de Tails desde la página oficial

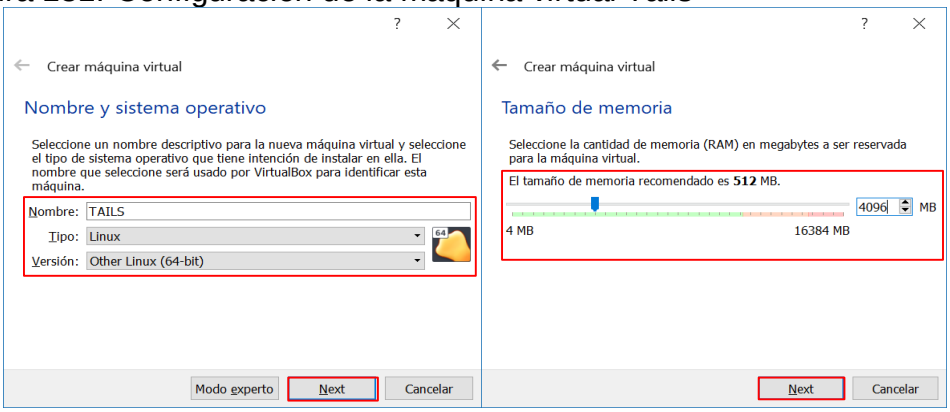


Fuente: El autor

[66] TAILS, Repositorio de descarga de TAILS 3.11, [En línea]. 2018 Disponible en: <https://tails.boum.org/install/download/index.en.html>.

En la Figura 131 se puede ver la creación de una máquina virtual, a la cual se le asignan un nombre nemotécnico, recursos de memoria, CPU y redes acordes con el sistema anfitrión, sin embargo, en el ítem de disco duro se elige la opción de archivo de disco duro virtual existente, y se busca el archivo ***tails-amd64-3.10.1.iso*** descargado previamente.

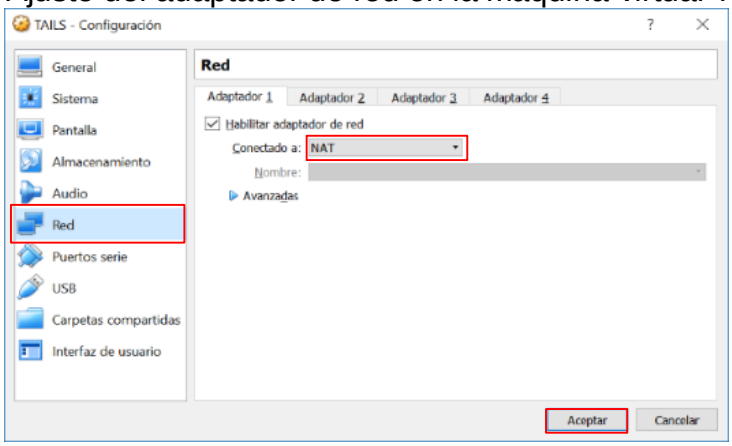
Figura 131. Configuración de la máquina virtual Tails



Fuente: El autor

Dado que la web profunda se considera un ambiente hostil es recomendable aislar la red interna de la máquina virtual. En este caso el adaptador de red quedara en modo NAT permitiendo establecer una conexión hacia internet, sin embargo, esta conexión esta aparte del host anfitrión y no existe comunicación entre ambas máquinas.

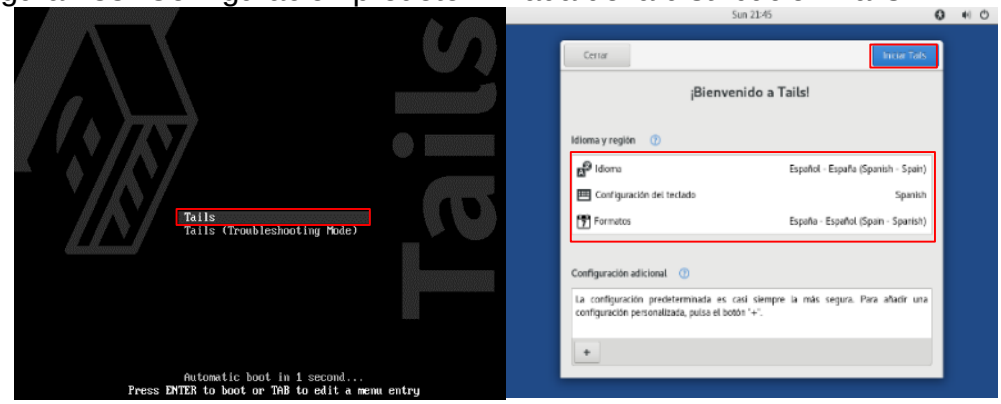
Figura 132. Ajuste del adaptador de red en la máquina virtual TAILS



Fuente: El autor

Con todas las configuraciones realizadas se procede seleccionar la máquina virtual *TAILS* y se inicia el sistema operativo, acto seguido se observa la secuencia de inicio validando servicios y configuraciones preestablecidas. En la Figura 133 se visualiza el mensaje de bienvenida a *Tails*, donde se puede configurar el idioma, la distribución del teclado y los formatos de codificación de caracteres.

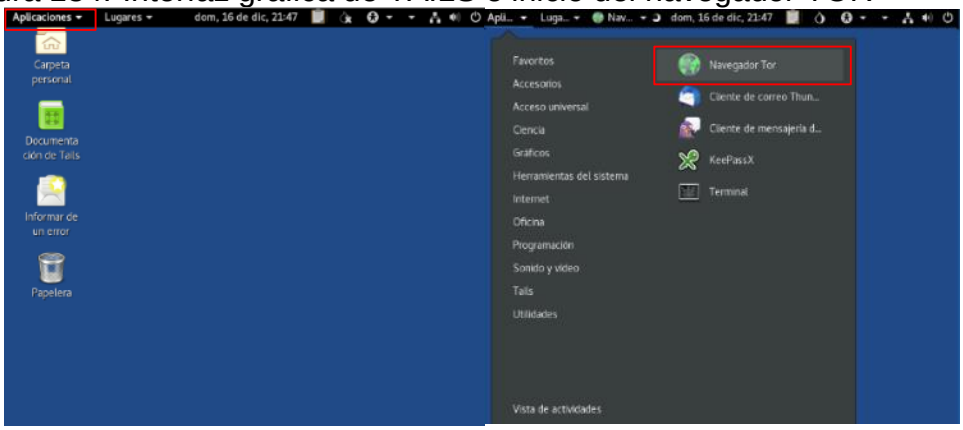
Figura 133. Configuración predeterminada de la distribución Tails



Fuente: El autor

En la Figura 134 se muestra la interfaz gráfica de la distribución Tails, para ejecutar el navegador Tor se debe ir a la opción ***Aplicaciones >> Navegador Tor*** y oprimir clic en el icono de Tor. El navegador empieza a cargar durante algunos segundos y cuando ya se encuentra listo para usar aparece un mensaje de bienvenida.

Figura 134. Interfaz gráfica de TAILS e inicio del navegador TOR



Fuente: El autor

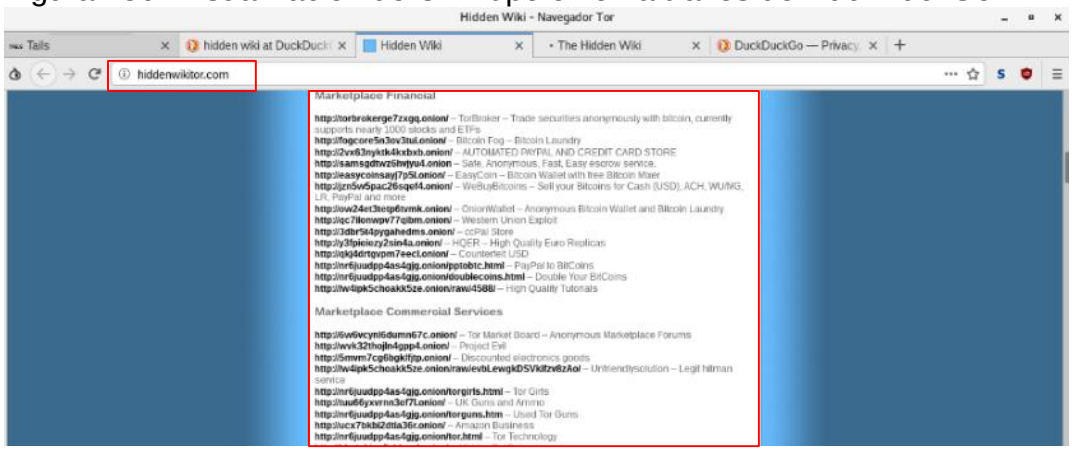
En la Figura 135 se observa que al ejecutar el navegador Tor se redirige a la página oficial de Tails, esto comprueba que la máquina virtual tiene salida a internet y puede ser usada para acceder a la Internet profunda.

Figura 135. Página principal de TAILS al ejecutar TOR

Fuente: El autor

Las URL en la *Deep Web* cambian constantemente y funcionan de manera diferente a comparación con los motores de búsqueda habituales, se utiliza el motor de búsqueda DuckduckGo para realizar una consulta sobre las URL de la *Hidden* Wiki. En la Figura 136 aparecen varios resultados de los cuales se debe validar e ingresar al que sea correspondiente al sitio que se desea visitar.

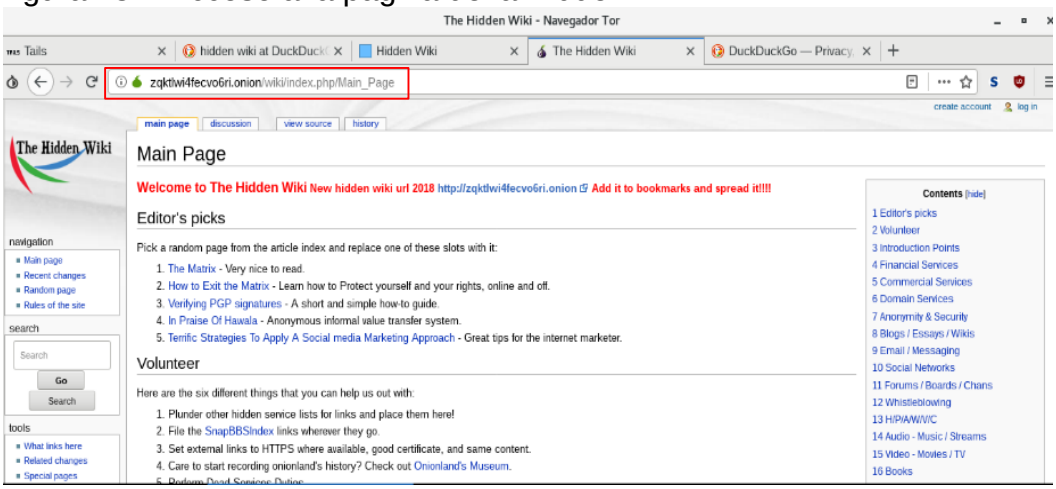
Figura 136. Visualización de URL tipo onion a través de DuckDuckGo



Fuente: El autor

En la Figura 137 se presenta la página web de la *Hidden* Wiki, en este sitio existe diferentes tipos de contenidos, al cual se recomienda ser precavido e ingresar puntualmente a lo que se requiere, porque este tipo de acceso a la red *Tor* requiere atención para no ingresar a contenido sensible o explícito.

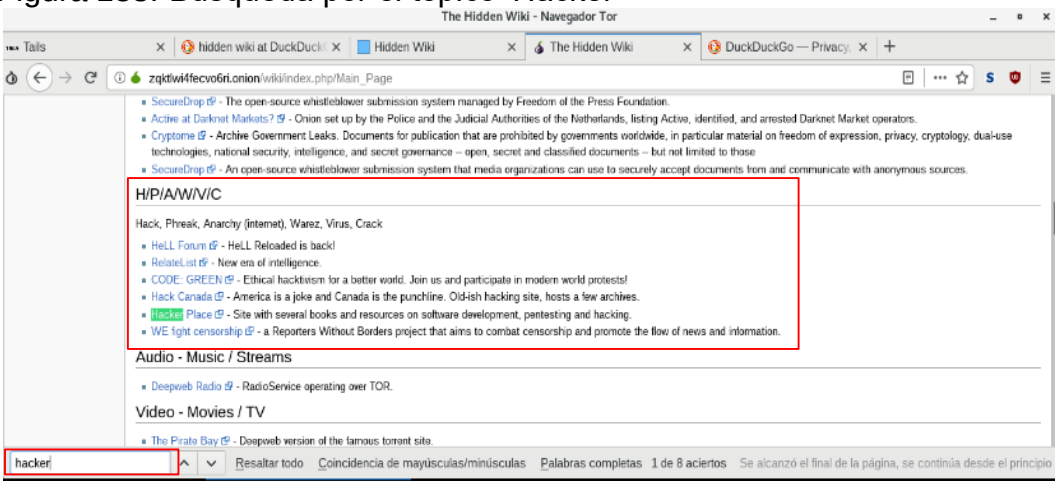
Figura 137. Acceso a la página de la Hidden Wiki



Fuente: El autor

En la Figura 138 se presenta la consulta del término "***Hacker"*** en la página de la *Hidden* Wiki, se observan diferentes *links* de acceso que ofrecen servicios profesionales y recursos relacionados con hacking.

Figura 138. Búsqueda por el tópico 'Hacker'



Fuente: El autor

6.3 ENFOQUE ADMINISTRATIVO

Debido a la reestructuración y crecimiento de la organización, es necesaria la vinculación de un consultor externo de seguridad de la información para la planeación, diseño, creación e implementación del Plan Estratégico de Seguridad de la Información (PESI), el cual se debe compartir con el nuevo responsable de ciberseguridad.

6.3.1 Diseño del plan estratégico de seguridad informática. La planeación estratégica de seguridad informática es la manera como se consiguen los objetivos TI por medio de la formulación de actividades estructuradas, de tal modo que, a través de herramientas tecnológicas, la organización se adapte a los cambios del entorno, se mantenga en operación y obtenga lucro en sus operaciones. El PESI está ligado con la toma de decisiones, la innovación y el valor agregado de las TIC para que la organización sea eficiente y genere beneficios económicos.

En el PESI se definen los objetivos que pretende alcanzar el área de tecnología, de tal modo que sean específicos, medibles, aceptables, reales y tengan un tiempo establecido. Con esto, se pueden adoptar acciones y asignar recursos que serán necesarios para alcanzar los objetivos previamente planteados. Dicho en otras palabras, el PESI define el camino a seguir, teniendo en cuenta lo que desea lograr y cómo se va a lograr. Entre otros, con el PESI se obtienen los siguientes aspectos clave:

- **Objetivos**: Definición formal y exacta de lo que se desea lograr o lo que se quiere conseguir.
- **Actividades**: Conjunto de pasos o acciones que se deben realizar para conseguir el objetivo.
- **Estrategias**: Definición formal y exacta de cómo se va a lograr el objetivo planteado.
- **Métricas**: Son valores numéricos para evaluar la eficiencia y resultados de las metas y estrategias.

El PESI es desarrollado para alinear la estrategia de ciberseguridad con los procesos críticos y los objetivos estratégicos de la organización, priorizando los proyectos más relevantes para mantener la seguridad de la información, la infraestructura tecnológica y la continuidad del negocio.

• **Tiempo estimado para el diseño del PESI.** El diseño del PESI es la definición del conjunto de proyectos y actividades que fortalecen la postura de una organización en materia de ciberseguridad, de tal modo que se dé prioridad a las acciones más relevantes para disminuir el impacto de los riesgos y se llegue a un estado aceptable.

El diseño del Plan Estratégico de Seguridad Informática para la empresa RANDOM S.A. está previsto para comenzar en el mes de octubre de 2019, con fecha de culminación el 28 de noviembre del mismo año, esto indica un total de 6 semanas calendario. En el Cuadro 7 están registrados los tiempos estimados y su cumplimiento depende directamente de la disponibilidad de recursos, personal y aprobaciones por parte de la gerencia.

Cuadro 7. Cronograma de actividades diseño del PESI

Actividad	**Semana**					
	1	**2**	**3**	**4**	**5**	**6**
	18 - 24 oct	**25 - 31 oct**	**1 - 7 nov**	**8 - 14 nov**	**15 - 21 nov**	**22 - 28 nov**
Inicio	X					
Ejecución						
Situación inicial de la organización	X					
Estrategia de la organización		X				
Definición de proyectos e iniciativas			X			
Clasificación de proyectos a ejecutar				X		
Valoración del riesgo				X	X	
Portafolio de proyectos					X	X
Cierre						
Aprobación del plan director						X
Fuente: El autor						

Este plan requiere de un análisis de la situación inicial de la organización y debe estar completamente acoplado con los objetivos estratégicos del negocio, además, debe incluir el alcance, definición de roles, responsabilidades y todo lo relacionado con buenas prácticas en cuanto a seguridad informática, el plan estratégico de seguridad se define con base en los siguientes aspectos:

- El tamaño de la organización o la cantidad de empleados.
- El nivel de madurez de la organización.
- El sector o campo de aplicación.
- Normatividad y aspectos legales.
- Naturaleza y medios de presentación de la información.
- Talento Humano.
- Nivel de confidencialidad de la información.
- Alcance del proyecto.
- Operaciones o procesos.
- Tecnología usada en las operaciones.

En el Cuadro 8 se describen las actividades de cada etapa y su correspondiente tiempo estimado, esto permite tener una visión clara de los tiempos de entrega y los entregables que deben presentarse a la gerencia.

Cuadro 8. Etapas y tiempo del plan estratégico de seguridad informática

Etapas	Descripción	Actividades
Situación inicial de la organización	Conocer e identificar la situación actual de la organización de cara a la postura de seguridad de la información, para esto se llevaban a cabo análisis de índole técnico, organizacional, normativo, administrativo, entre otros. Es la fase más compleja e importante porque se involucran el personal de diferentes áreas y su objetivo es definir el nivel de madurez de seguridad. Actividades previas: establecer el alcance, definir responsables de la gestión de los activos, realizar la valoración preliminar y establecer los objetivos.	• Ejecutar entrevistas con las partes interesadas (directivos y/o dueños de procesos). • Comprender la infraestructura de TI que soporta el negocio. • Consultar y analizar los objetivos estratégicos, misión y visión. • Consultar y analizar la documentación de seguridad de la información, planeación • estratégica, riesgos y/o continuidad (si existieran). • Identificar los requerimientos regulatorios.
Estrategia de la organización	Es necesario conocer los proyectos que se están ejecutando actualmente, posibles crecimientos o cambios en la organización. En este punto es importante tener en cuenta si los servicios TI son propios o de terceros con un proveedor externo. Este tipo de consideraciones puede influir en la dirección del plan de seguridad y rigen las medidas a implementar. A partir de este punto el plan se alinea con los objetivos de la organización, por lo tanto, la estrategia, los roles, responsables e interesados son factores clave para obtener una visión objetiva y global del negocio.	• Conocer los planes de aseguramiento existentes. • Conocer las proyecciones de seguridad. • Identificar estado de madurez de la seguridad informática. • Análisis técnico de seguridad. • Análisis de riesgos. • Identificar los objetivos de la estrategia de Seguridad Informática • Establecer la relación entre los objetivos organizacionales y los objetivos de la estrategia de seguridad informática.

Cuadro 8. (Continuación)

Etapas	Descripción	Actividades
Definición de proyectos e iniciativas	Con la información recolectada en etapas previas, se procede a definir las acciones, actividades e iniciativas de proyectos para conseguir un grado óptimo de seguridad en la organización. Se parte del punto de iniciativas encaminadas a mejorar los procedimientos y que presentan deficiencias o no conformidades en sus controles establecidos, según un marco legal, regulatorio o normativo. Después se llevan a cabo todas aquellas acciones relacionadas con la definición y especificación de controles técnicos, administrativos que tienen o pueden ser mejorados.	• Asociar las iniciativas del portafolio de proyectos a los objetivos de seguridad. • Análisis financiero de los proyectos e iniciativas, las cuales están en función del tiempo y contemplan recursos de índole locativo, administrativo y tecnológico. • Definir los proyectos para gestionar el riesgo residual y mantenerlo estable o en un grado aceptable.
Clasificación de proyectos a ejecutar	Con el listado de proyectos, iniciativas y actividades se procede a clasificarlos dependiendo su nivel de prioridad, en esta fase se agrupan las propuestas para tener un catálogo de opciones homogéneo, donde se puede establecer el origen, cumplimiento legal, análisis técnico o de riesgos, estos aspectos pueden ayudar a la clasificación y agrupamiento dependiendo la naturaleza del proyecto.	• Asociar las iniciativas del portafolio de proyectos a los objetivos de seguridad. • Es recomendable que también se considere la prioridad en función del esfuerzo y los recursos requeridos para desarrollar el proyecto.
Valoración del riesgo	Realizar el análisis de riesgos basado en la metodología de gestión de riesgos MAGERIT.	• Identificar los activos de información. • Identificar vulnerabilidades y amenazas asociadas. • Proponer las salvaguardas.
Portafolio de proyectos	Definir el portafolio de proyectos con los esfuerzos priorizados de acuerdo al contexto organizacional y basado en las diferentes capas de protección.	• Realizar el documento base de proyectos de seguridad informática.
Aprobación del plan director	Con la versión preliminar el plan director de seguridad se puede remitir a la alta gerencia para su correspondiente revisión y aprobación. Aunque también puede modificarse su alcance, prioridad y duración de algunos proyectos, considerando la gerencia, por ende, puede ser un proceso cíclico hasta que se cuente con la versión final del plan y que esté aprobada formalmente por la gerencia.	• Divulgar la versión final del plan director de seguridad a todos los colaboradores de la organización, de tal modo que se materialicen las proyectos, iniciativas y actividades mencionadas.

Cuadro 8. (Continuación)

Etapas	Descripción	Actividades
Puesta en marcha	El PESI es la hoja de ruta para alcanzar el nivel de seguridad esperado y que necesita la organización para el desarrollo de la misión, visión y los procesos críticos del negocio. Dada la complejidad y magnitud del plan, es pertinente abordarlo similar a un proyecto, el cual debe ser diseñado y desarrollado bajo una metodología de gestión de proyectos como PMI (*Project Management Institute*). La participación de la alta gerencia y los colaboradores garantizan el éxito de plan director.	Aspectos claves del plan director de seguridad, son: • Presentación general del proyecto a todo el personal. • Asignación de roles y responsabilidades a cada proyecto, por medio de un comité de gestión y supervisión. • Seguimiento periódico de los proyectos y del plan director. • En cada momento clave del plan director se llevan auditorias para verificar la remediación de debilidades y deficiencias.
Fuente: El autor		

6.3.1.1 Riesgos inherentes del PESI. El riesgo inherente es esencial y permanece durante todo el proyecto porque forma parte de las actividades, dicho en otras palabras, es el riesgo que no se puede determinar o eliminar porque está implícito en cada etapa del proyecto; en la Tabla 6 se identifican un conjunto de riesgos inherentes del PESI.

Tabla 6. Riesgos inherentes del PESI

Tipo de riesgo	Descripción
Nivel de cumplimiento	• Desafíos para identificar roles, tecnologías y mercados en el ecosistema digital de la organización. • Aparición de nuevas tecnologías o exigencias en cuanto a ciberseguridad y/o privacidad de la información. • Incumplimiento de la regulación legal y normatividad técnica vigente.
Nivel operacional	• Incumplimiento de métricas asociadas al desempeño y ejecución de procesos en contraste con los planes. • Desafíos para mejorar los procesos críticos y misionales. • Tratamiento de la información relacionada con el negocio.
Nivel Financiero	• Iliquidez, agotamiento de recursos económicos durante el periodo de definición o implementación. • Incremento de la moneda internacional que impacte en el costo total del proyecto.
Nivel de Estratégico	• Deficiencias en la supervisión de las fases del proyecto. • Fallos no intencionados o errores humanos.
Fuente: El autor	

6.3.1.2 Proyección del costo del diseño del PESI. La viabilidad del PESI está directamente relacionado con del tamaño de la organización y los recursos necesarios para llevarlo a cabo, teniendo presente los costos de diseño. Se dividieron los recursos en 3 aspectos: talento humano, recurso técnico y otros recursos. El desarrollo de este punto tiene como precedente una organización de tamaño mediano, donde el PESI está planteado para ser diseñado en máximo 6 semanas, con 48 horas semanales laborales, obteniendo la cantidad de 288 horas. En cuanto al talento humano requerido para la ejecución del proyecto se estiman 2 perfiles de cargo correspondientes al oficial de la seguridad de la información y al analista de ciberseguridad, en el Cuadro 9 se estima el valor total del recurso humano y se describe brevemente las funciones de cada rol.

Cuadro 9. Valor total del talento humano

Tipo	Descripción	Valor hora	Cantidad	Valor total
Oficial de seguridad de la información	Colaborador encargado de diseñar el PESI tiene contacto directo con la gerencia.	17.000 pesos	288 horas	4.896.000 Pesos
Analista de Ciberseguridad	Profesional encargado de apoyar la documentación, realizar auditorías, establecer métricas.	13.000 pesos	288 horas	3.744.000 Pesos
Talento Humano				**8.640.000 Pesos**
Fuente: El autor				

En el Cuadro 10 están registrados los costos asociados a otros recursos como material, papelería y transporte. En cuanto a los recursos tecnológicos y locativos necesarios para el diseño del PESI, estos son propiedad de la organización, por lo tanto, no se tendrán en cuenta a nivel presupuestal, pero se listan a continuación a manera de referencia:

- Equipos computacional y ofimático.
- Impresora.
- Instalaciones físicas.
- Acceso a Internet.
- Servicio de correo electrónico.
- Gastos administrativos.
- Logística.
- Otros gastos.

Cuadro 10. Valor total de otros recursos

Tipo	Descripción	Valor unitario	Cantidad	Valor total
Capacitaciones	Sensibilización y divulgación de la norma ISO 27001	250.000 Pesos	3	750.000 Pesos
Material de la norma ISO 27001:2013	Documentación, libros y textos relacionados con la norma ISO 27001.	300.000 Pesos	1	300.000 Pesos
Papelería	Fotocopias, impresiones, resmas de papel, discos compactos, etc.	200.000 Pesos	1	200.000 Pesos
Transporte	Visitas al cliente	300.000	1	300.000 Pesos
Total de otros recursos				**1.550.000 Pesos**

Fuente: El autor

Con base en la anterior estimación del valor que representa el diseño del PESI, se puede concluir que la asignación de 2 especialistas más otros gastos durante 6 semanas tiene un costo estimado de 10.699.500 pesos en moneda corriente, en la Tabla 7 se registra el costo total de la propuesta.

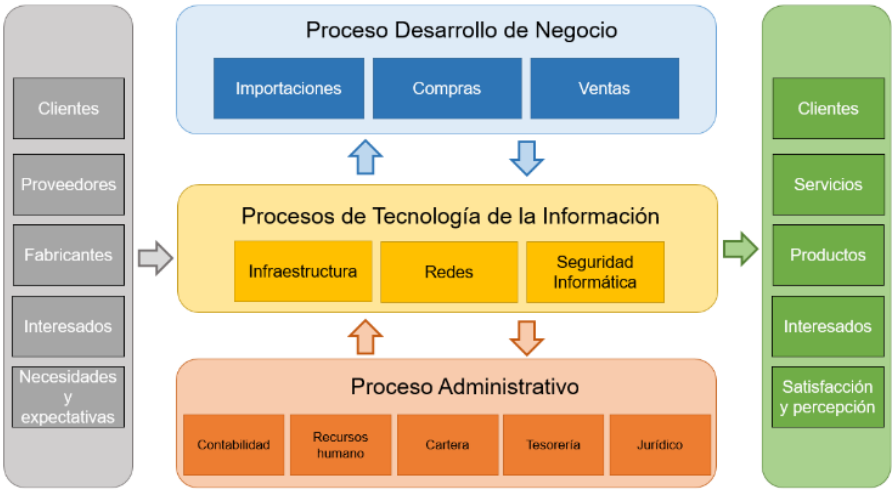
Tabla 7. Costo general del diseño del PESI

Recurso	Valor total
Total recursos humanos	8.640.000 Pesos
Total otros recursos	1.550.000 Pesos
Costos imprevistos (5%)	509.500 Pesos
Costo Total	**10.699.500 Pesos**

Fuente: El autor

6.3.1.3 Estructura organizacional. Es la distribución interna y administrativa que tiene una organización para definir la serie de procesos con sus correspondientes áreas de trabajo que se encargan de la operación. Esta representación gráfica de la estructura empresarial ofrece una visión global de la composición de la empresa y como interaccionan las diferentes dependencias para lograr los objetivos del negocio, en la Figura 139 se observan los diferentes procesos de la empresa RANDOM SA.

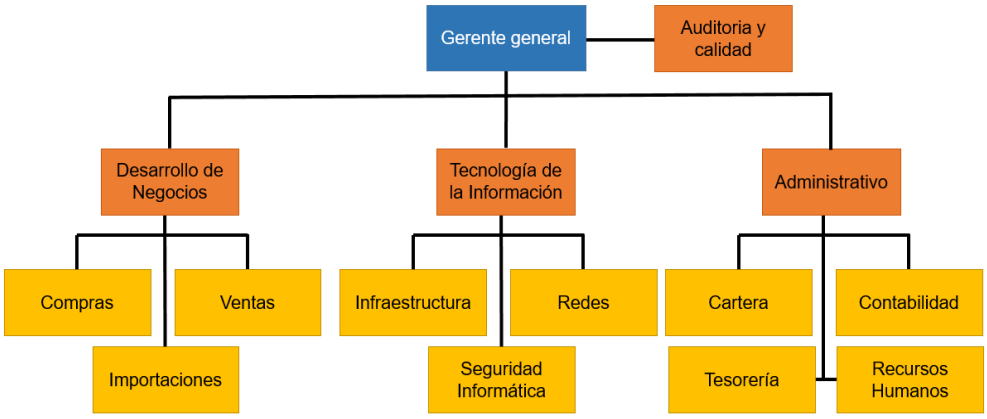
Figura 139. Procesos de RANDOM S.A.



Fuente: El autor

La organización RANDOM S.A, cuenta con un total de 58 colaboradores distribuidos entre personal administrativo, operativo y gerencial. En la Figura 140 se muestra la estructura jerárquica de las diferentes áreas y la relación con los procesos críticos de la organización.

Figura 140. Organigrama de RANDOM S.A.



Fuente: El autor

Al realizar un acercamiento al departamento TI, se encuentran las diferentes áreas encargadas de atender la infraestructura, las redes y la seguridad informática al interior de la empresa RANDOM S.A. En la Tabla 8 se describen las funciones que tienen asignadas cada área.

Tabla 8. Funciones de las áreas del departamento TI

Área	Descripción
Infraestructura	• Brindar soporte interno en la organización. • Soportar la infraestructura de los servicios contratados. • Compra, configuración e instalación de equipos de cómputo, laptops, servidores, periféricos y demás elementos necesarios para soportar la infraestructura tecnológica. • Gestión del directorio activo y cuentas de correo.
Redes	• Gestionar los servicios de telecomunicaciones contratados por los clientes. • Implementación de soluciones de Networking para clientes. • Operar el *Network Operations Center* (NOC). • Capacitación a las empresas en temas de redes. • Aplicación de controles de seguridad para los servicios de comunicaciones. • Soporte de los servicios contratados. • Mantenimiento de computadores (sólo equipos propiedad del Centro).
Seguridad Informática	• Generación de conceptos técnicos para tramitar baja de equipos. • Realiza copias de seguridad de los sistemas de información y servidores virtuales que se encuentran en el Departamento de Sistemas.

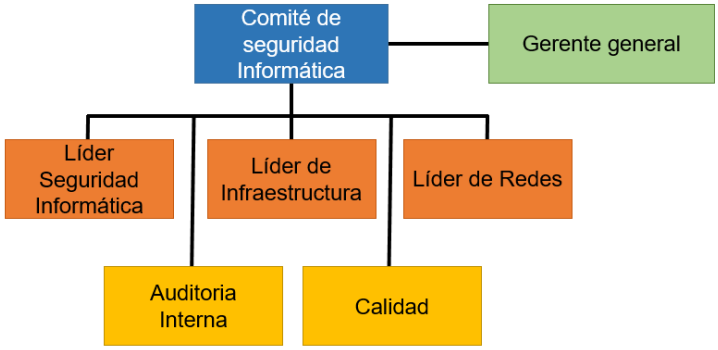
Fuente: Enunciado del enfoque administrativo, curso de proyecto de seguridad informática II.

Con la nueva contratación se espera fortalecer el área de seguridad informática de modo que este subproceso se convierta en un aliado estratégico de los demás procesos y subprocesos, para salvaguardar la información crítica, sensible y valiosa de la organización. Además, esta persona será uno de los principales actores en el comité de seguridad informática y sobre este colaborador recae la estrategia de ciber-seguridad de la organización.

- **Reestructuración del comité de seguridad informática.** La seguridad de la información es un proceso continuo y transversal entre las áreas que componen una organización, por lo tanto, es necesario definir los roles, funciones y responsabilidades de los profesionales encargados de velar y asegurar y salvaguardar la información confidencial, critica, sensible y valiosa de la organización.

El comité de seguridad informática está conformado por un grupo interdisciplinario que tiene poder de decisión, ya que es la máxima autoridad en materia de ciberseguridad al interior de la organización. En la Figura 141 se presenta la estructura del comité de seguridad informática, el cual gira en torno al departamento TI y sus áreas de apoyo.

Figura 141. Estructura del comité de Seguridad Informática



Fuente: El autor

- Definir el alcance y los límites del SGSI, en función de los objetivos del negocio. Es necesario identificar el contexto de la organización, la ubicación geográfica, los activos de información y la tecnología utilizada.

- Establecer la metodología de análisis y gestión del riesgo que sea apropiada para el SGSI, a los requisitos legales, operacionales y contractuales.

- Inspeccionar, vigilar y controlar la implementación y adopción del SGSI, estableciendo un proceso de mejora continua. Definir y aprobar la declaración de aplicabilidad propuesta por el SGSI.

- Elaborar el plan para el tratamiento de riesgos para identificar las acciones pertinentes, los recursos necesarios, roles, responsabilidades y prioridades para tratar los riesgos de seguridad de la información oportunamente.

- Gestionar la adquisición de recursos idóneos y necesarios para el SGSI para mejorar la seguridad de la información en la organización. Verificar la efectividad del SGSI, teniendo en cuenta los resultados de las auditorias de seguridad, métricas, incidentes, eventos, indicadores y retroalimentación de las partes interesadas.

- Conocer los procedimientos y controles para dar respuesta oportuna a los eventos e incidentes de seguridad. Revisar y vigilar los planes de seguridad informática propuestos y en ejecución.

- Incentivar iniciativas sobre seguridad de la información y revisar periódicamente los indicadores del SGSI.

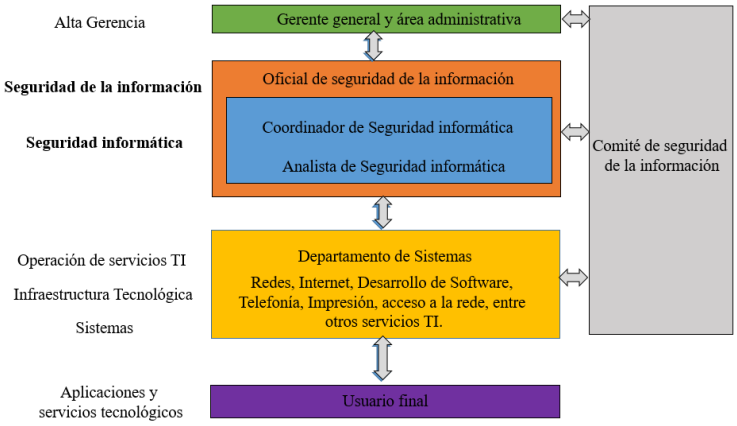
- Publicar comunicados a la organización e incentivar campañas de sensibilización con respecto a la importancia de la seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continua.

- Evaluar los criterios para aceptar los riesgos y que niveles de riesgo son aceptables en la organización. Garantizar la ejecución de auditorías internas del SGSI en intervalos periódicos de tiempo, así como la divulgación de los resultados.

- Establecer el procedimiento de asignación de responsabilidades y roles definidos en el SGSI, para que todo el personal sea competente al realizar las actividades.

Dentro del marco del comité de seguridad informática, es necesario definir roles para cada uno de los responsables o encargados de la seguridad de la información, de tal modo que se asignen un conjunto de funciones específicas y se lleven a cabo los proyectos propuestos. Vale la pena resaltar que la seguridad de la información es una responsabilidad de todos los colaboradores de la organización, en la Figura 142 se observa cómo está conformado el comité de seguridad informática.

Figura 142. Composición del comité de seguridad informática



Fuente: El autor

Con base en el comité de seguridad informática, es importante definir los perfiles de cargo para cada área, por lo tanto, en los Cuadros 11, 12 y 13 se detallan las características de los principales roles relacionados con la seguridad de la información en la organización.

Cuadro 11. Perfil del oficial de seguridad de la información

Oficial de seguridad de la información, privacidad y cumplimiento	
Competencias	
Formación	Profesional universitario de ingeniería (sistemas, electrónica) o administración. Conocimientos en la norma ISO 9001:2015, auditor Interno o Líder ISO – 27001:2013 Conocimientos en la normativa relacionada con ciberseguridad, protección de datos y gestión de riesgos.
Experiencia	Mínimo 5 años en el área de informática, 2 de estos en gestión seguridad de la información. Gestión de incidentes de seguridad, riesgos informáticos y continuidad del negocio.
Habilidades	• Trabajo en equipo. • Capacidad de escucha y análisis. • Análisis de situaciones y resolución de problemas. • Alta capacidad de aprendizaje. • Redacción y presentación de documentos. • Redactar y presentar documentos e informes. • Orientación de servicio al cliente.
Responsabilidades	
• Vigilar el cumplimiento de la documentación del SGSI. • Definir el alcance, la política y objetivos del SGSI de la organización, en conjunto con la dirección. • Comunicar oportunamente las novedades y actualizaciones del SGSI. • Acoplar los objetivos estratégicos con los requerimientos de los sistemas de gestión de la organización. • Elegir los controles, técnicas y procedimientos necesarios para gestionar los riesgos. • Crear el comité de respuesta a incidentes de seguridad, para atender los problemas relacionados a la seguridad de la información dentro de la organización. • Definir los recursos humanos, físicos, tecnológicos y económicos requeridos para el establecimiento mantenimiento y mejoramiento continuo.	
Funciones	
• Promover la aplicación de auditorías a los sistemas de gestión, para evaluar las prácticas y cumplimiento legal, normativo y contractual. • Desarrollar procedimientos específicos que fortalezcan la política de seguridad informática. • Diseñar y aplicar una metodología de análisis de riesgo para evaluar los sistemas de gestión en la organización. • Diseñar, implementar y mantener el procedimiento para la gestión de Incidentes de seguridad de la información. • Crear y actualizar las políticas de seguridad informática, con base en el descubrimiento de nuevos riesgos y amenazas. • Determinar los requisitos y recursos para la gestión optima de la seguridad de la información. • Desarrollar un plan de capacitación y sensibilización relacionado con buenas prácticas y adopción de seguridad de la información. • Desarrollar, actualizar y gestionar las estrategias para la continuidad del negocio.	
Fuente: El autor	

Cuadro 12. Perfil del coordinador de seguridad informática

<table>
<tr><th colspan="2">Coordinador de Seguridad Informática</th></tr>
<tr><th colspan="2">Competencias</th></tr>
<tr><td>Formación</td><td>Profesional en el área de ingeniería de sistemas, electrónico o telemática Especialización y/o maestría seguridad de la información, informática o proyectos.
Certificación CISSP, CISM y/o auditor líder ISO 27001.
Con conocimientos en estándares ISO 9001, ISO27001, ITIL, PCI.</td></tr>
<tr><td>Experiencia</td><td>Mínimo 4 años en áreas de seguridad de la información, informática y/o infraestructura. Experiencia liderando la ejecución de proyectos o servicios en tecnologías de información y comunicación o afines</td></tr>
<tr><td>Habilidades</td><td>• Trabajo en equipo.
• Recursividad, creatividad e iniciativa.
• Capacidad de escucha y argumentación.
• Alta capacidad aprendizaje.
• Orientación a resultados.
• Orientación al cliente.
• Capacidad Investigativa y recursividad.
• Liderazgo y manejo de personal.
• Habilidad de Negociación.
• Habilidad gerencial y comunicativa</td></tr>
<tr><th colspan="2">Responsabilidades</th></tr>
<tr><td colspan="2">• Cumplir con los lineamientos y directrices definidos en el SGSI.
• Mantenerse capacitado y actualizado respecto del entorno tecnológico y específicamente en las soluciones contenidas en el portafolio de la compañía, a través del autoaprendizaje, aprendizaje entregado por la compañía y/o aprendizaje entregado por los socios de negocio.
• Identificar y reportar oportunidades de negocio en los clientes.
• Apoyar las estrategias y tareas de mercadeo desarrolladas para la consecución de los objetivos corporativos.
• Realizar el registro continuo de tareas, soportes, reuniones, base de conocimiento y en general toda información que se genere de la relación técnica con los clientes.
• Proponer y documentar nuevos formatos, procedimientos, políticas, estándares y guías que mejoren la prestación de los servicios y/o proyectos y el cumplimiento de la ISO 27001.</td></tr>
<tr><th colspan="2">Funciones</th></tr>
<tr><td colspan="2">• Garantizar el desarrollo y oportunidad de procedimientos, formatos y documentos en general requeridos para soportar la prestación de los servicios del área.
• Garantizar el nivel técnico del grupo que integra la gerencia de ciberseguridad para la ejecución de sus funciones.
• Asegurar la capacitación y entrenamiento permanente en las soluciones y servicios definidos en el portafolio de la empresa, bien sea que ésta sea entregada por la compañía, los socios de negocio u obtenida directamente
• Revisar y presentar periódicamente a la alta gerencia un informe con los incidentes, problemas o inquietudes técnico-comerciales más frecuentes y generar las acciones correspondientes.
• Promover la creación de documentación o manuales que alimenten la base de datos de conocimiento.</td></tr>
<tr><td colspan="2">Fuente: El autor</td></tr>
</table>

Cuadro 13. Perfil del analista de seguridad informática

Analista de Seguridad Informática	
Competencias	
Formación	Profesional en el área de ingeniería de sistemas, electrónico, telemática o afines, con estudios adicionales como diplomados o especialización en seguridad, proyectos, redes, entre otros. Conocimientos en redes e infraestructura, sistemas Windows y Linux.
Experiencia	Mínimo 2 años en el área de informática y/o seguridad de la información. Atención de eventos e incidentes de seguridad a clientes internos y externos, preferible experiencia laboral con un proveedor de servicios de seguridad gestionada.
Habilidades	• Trabajo en equipo. • Recursividad, creatividad e iniciativa. • Capacidad de escucha y argumentación. • Alta capacidad aprendizaje. • Orientación a resultados. • Orientación al cliente.
Responsabilidades	
• Conocer las soluciones y servicios de la compañía, especialmente los relacionados con la prestación de servicios tecnológicos. • Replicar el entrenamiento recibido en cualquiera de las áreas. • Apoyar las estrategias y tareas desarrolladas para la consecución de los objetivos. • Realizar un manejo responsable y ético de las herramientas entregadas por la organización tales cómo: bases de datos, información que se encuentra en la herramienta de documentación de uso corporativo, elementos de hardware y software, entre otros; para el cumplimiento de las tareas y velar por mantener la protección de los datos suministrados y los pilares de la seguridad informática; confidencialidad, integridad, disponibilidad, privacidad y trazabilidad.	
Funciones	
• Cumplir con el plan de entrenamiento y evaluación establecido por la gerencia de ciberseguridad. • Asegurar la capacitación y entrenamiento permanente en las soluciones y servicios definidos en el portafolio de la empresa, bien sea que ésta sea entregada por la compañía, los socios de negocio u obtenida directamente. • Reportar cualquier incidente de seguridad y actualizar la base de conocimientos. • Dar soporte y solución oportuna a los incidentes y problemas reportados por los usuarios internos y clientes externos de acuerdo con los SLA´s convenidos 7X24. • Determinar y solicitar el apoyo de los jefes inmediatos u otra(s) dirección(es) para mantener el curso y el cumplimiento de los tiempos en la prestación de los servicios contratados por parte del cliente. • Realizar análisis proactivo y escalamiento de las alarmas identificadas por las herramientas de gestión y monitoreo. • Escalar los incidentes y requerimientos teniendo en cuenta el nivel de prioridad y los tiempos establecidos en los acuerdos de servicio. • Informar periódicamente al coordinador ciberseguridad y al siguiente nivel de escalamiento, los incidentes o problemas más frecuentes para generar un problema o documento para entregar a los clientes y minimizar el registro de casos.	
Fuente: El autor	

- **Importancia del PESI en la organización.** El PESI (Plan Estratégico de Seguridad Informática), es la firme intención que tiene la gerencia para desarrollar proyectos de seguridad informática con la finalidad de proteger y salvaguardar los diferentes activos de información en la organización. Este plan establece las prioridades, actividades, criticidad, funciones, roles y recursos necesarios para tener una estrategia de ciberseguridad que mejore el nivel de madurez en materia de ciberseguridad.

Los proyectos que se abordan en un plan estratégico de seguridad informática van desde el aspecto técnico, administrativo, legal o del negocio, para lo cual, previamente se debe definir la situación actual y el contexto de seguridad de la información en la organización y con esto identificar posibles iniciativas y mejorar los procesos de gestión y tratamiento de los activos de la información. En cada proyecto se establece qué se va a proteger y el modo como se va a proteger, para lo cual se plantean las actividades, métodos o mecanismos necesarios; otro aspecto clave son los diferentes escenarios y riesgos que se pueden mitigar con las acciones de cada proyecto.

- **Objetivos del PESI.** Son las metas fijadas por el comité de seguridad informática para el desarrollo de las diferentes iniciativas en materia de protección de datos, privacidad y seguridad de la información.

  - **General.** Establecer el PESI (Plan Estratégico de Seguridad Informática), que permita especificar los planes de acción para alcanzar una arquitectura de seguridad con niveles de madurez óptimos, bajo un entorno de riesgo aceptable.

  - **Específicos**
    - Dar continuidad a la gestión de la estrategia de ciberseguridad para apoyar al encargado de seguridad de la información una vez se incorpore a la organización.

    - Definir la arquitectura de seguridad informática, (políticas, procedimientos, estructuras e infraestructura), apoyado con buenas prácticas metodológicas como MAGERIT, ISO 27001, OSSTMM, etc.

    - Definir el plan de implementación de la arquitectura a través del establecimiento objetivos y planes de acción (programas, proyectos e iniciativas) a 3 años para alcanzar un nivel de madurez óptimo y en un entorno de riesgo aceptable.

    - Definir la estrategia de ciberseguridad que permita asegurar el cumplimiento del plan estratégico de seguridad informática.

- Alinear los objetivos de seguridad de la información con los objetivos de la organización, desarrollando el plan estratégico de seguridad PESI.

- Desarrollar la cultura organizacional en protección de datos personales y seguridad de la información.

- Mantener el cumplimiento regulatorio relacionado con seguridad de la información.

- Evaluar el nivel de seguridad y exposición de activos a través de análisis de riesgos, además, apoyar la remediación de las vulnerabilidades y brechas encontradas a través de esas actividades.

6.3.1.4 Alcance del PESI. El Plan Estratégico de Seguridad Informática para RANDOM S.A., permite el acoplamiento y la cohesión de los objetivos de seguridad Informática con las operaciones del negocio. Partiendo del análisis de riesgos se identifica la probabilidad (frecuencia) e impacto (magnitud) de la materialización de amenazas, de tal modo que se dé prioridad a las actividades en función de las necesidades organizacionales, operativas y requerimientos legales, normativos o contractuales.

El PESI se aplica de manera transversal para todos los recursos tecnológicos y es de carácter obligatorio su cumplimiento de parte de todos los usuarios que tengan algún tipo de vínculo o relación con los activos de la información. Se precisa especial seguimiento para los diferentes proyectos en función de los niveles de información confidencial.

6.3.1.5 Situación inicial de la organización. La información propia y de los clientes es considerada un activo sumamente importante para el cumplimiento de la misión y los objetivos corporativos, por lo cual es pertinente la implementación reglas y medidas que protejan la confidencialidad, integridad, privacidad y disponibilidad de la información durante todo el ciclo de vida de los datos. Las herramientas, soluciones y medidas implementadas permiten adoptar las mejores prácticas de la industria para dar cumplimiento a los requisitos fundamentales de negocio y del sistema de gestión de seguridad de la información (SGSI).

- **Reseña:** RANDOM S.A provee la infraestructura de telecomunicaciones necesaria para la prestación de servicios de Internet móvil y cableado, así como gestión de dispositivos activos, los cuales son utilizados en actividades de diferentes sectores, apoyando a las empresas de los segmentos empresarial y Pyme a enfrentar los desafíos y necesidades del mercado mediante la prestación de servicios y comercialización de

soluciones TIC. De igual forma, se cuentan con aliados estratégicos y socios de negocios en múltiples empresas líderes de la industria de telecomunicaciones, con lo cual se ha logrado posicionamiento empresarial, liderazgo y reconocimiento acerca dentro del foco de negocios.

- **Misión:** Proveer servicios y productos innovadores de alta calidad, que estén relacionados con las tecnologías de la información y las telecomunicaciones, haciendo más rentable y productivo el negocio de nuestros clientes.

- **Visión:** Obtener reconocimiento de parte nuestros clientes como un aliado de valor que les permite mejorar su negocio por medio del suministro de productos y servicios que ayuden el cumplimiento de sus objetivos misionales.

- **Valores Corporativos.** La cultura organizacional promueve las siguientes características y habilidades en todos los colaboradores:

  - **Respeto**: Aceptar siempre que las ideas, expresiones o posiciones propias pueden ser diferentes a las de los otros, ver el valor en las diferencias y tener la capacidad de construir sobre estas.

  - **Honestidad**: Enfrentar todas las situaciones y errores aun cuando tengamos que reconocer ante otras personas que los hemos cometido y estos nos causen problemas.

  - **Compromiso**: Hacerse cargo de las obligaciones y sus impactos, para conseguir sacar adelante un proyecto y alcanzar los objetivos por encima de lo que se espera.

  - **Orientación al cliente**: Tener una actitud permanente para detectar, comprender y satisfacer las necesidades de nuestros clientes, así como realizar esfuerzos para de sobrepasar las expectativas.

  - **Comunicación efectiva**: Escuchar de forma atenta, proactiva y asertiva para comprender al otro y expresar las ideas en forma oportuna, clara, directa y respetuosa para lograr los objetivos planteados.

  - **Trabajo en equipo**: Buscar el logro de objetivos comunes de forma coordinada, activa, solidaria y creativa de tal manera que se aprovechen las sinergias para obtener los mejores resultados posibles.

- **Localización:** Actualmente la oficina administrativa de RANDOM S.A. se encuentra localizada en la ciudad de Bogotá en un prestigioso barrio al norte de la ciudad. Su centro de datos se encuentra ubicado en el datacenter ubicado en el municipio de Tocancipa Cundinamarca, este datacenter que cuenta con la certificación TIER III, estándar reconocido a nivel mundial para centro de datos.

- **Infraestructura tecnológica:** Está compuesta por el hardware y software que soporta los diferentes servicios tecnológicos de la organización:

    - Equipos de usuarios final.
    - Servidores y centro de datos
    - Equipos de comunicaciones.
    - Equipos de seguridad.
    - Impresoras.
    - Cableado estructurado.
    - Puntos de acceso inalámbrico.
    - Telefonía.
    - Aplicaciones.

- **Sistemas de información:** Para alcanzar los objetivos organizacionales se cuenta con aplicaciones especializadas, asimismo una aplicación CRM para la gestión de casos y de clientes. Adicionalmente se cuenta con aplicaciones de ofimática, correo electrónico y organización documental que apoya las actividades y los procesos de la organización.

Objetivos estratégicos del departamento TI

- **Infraestructura:** Mantener la infraestructura técnica de los centros de datos y puestos de trabajo requerida y acorde a las mejores prácticas de la industria. Actualizar constantemente el esquema de seguridad para tecnologías de la información.

- **Redes:** Garantizar la efectiva prestación de los servicios contratados con nuestros clientes. Ofrecer una administración confiable y oportuna de los servicios de telecomunicaciones.

- **Seguridad informática:** Velar por la integridad, disponibilidad y confidencialidad de la información y los servicios de telecomunicaciones.

- **Recursos humanos:** Se cuenta con una planta de recurso humano con una combinación de conocimientos y habilidades para llevar a cabo los avances y logros de la organización, la selección de este personal se realiza de acuerdo con lo establecido en el procedimiento de contratación.

Adicionalmente se dispone de recursos para garantizar la preparación y conocimientos adicionales que se van adquiriendo mediante cursos y otros mecanismos, posteriores al entrenamiento recibido.

La notación de "***Seguridad Informática***" y no de "***Seguridad de la Información***", representa el alcance del proyecto el diseño de un plan estratégico sobre los activos de TI controlados por el Departamento de Tecnología, dejando de lado la documentación en papel, las comunicaciones escritas y verbales.

- **Estado actual.** En la actualidad, RANDOM S.A. está en busca de certificar sus procesos en normas internacionales para conocer el estado actual de la seguridad de la información, garantizar que su catálogo de servicios cumple y excede las expectativas de sus clientes, además esta organización tiene una proyección de incorporarse en nuevos mercados, para lo cual requiere implementar un SGSI (Sistema de Gestión Seguridad de la información), debido a que no cuentan con este tipo de documentación formal. En vista de lo anterior, se requiere desarrollar el análisis de riesgos contemplando la metodología de riesgos MAGERIT, esto sirve como insumo para proponer e implementar el SGSI en la organización.

  - El centro de datos cuenta con 2 aires acondicionados mini Split de 1200 BTU y se les hace mantenimiento preventivo 1 vez al año.

  - En los últimos 2 años se han generados perdida de datos debido a empleados inconformes.

  - La segmentación de la red no se ha documentado por lo cual cada vez que hay un inconveniente se debe invertir mucho tiempo.

  - Los equipos perimetrales UTM Fortigates internos de la compañía no tienen reglas definidas ni licencia de uso.

  - Los computadores portátiles no cuentan con cifrado en disco duro.

  - La organización no cumple con los requerimientos de seguridad de la Ley 1581 de 2012 de protección de datos personales.

6.3.1.6 Análisis de riesgos. El PESI es la definición y prelación de proyectos de seguridad enfocados en disminuir los riesgos asociados a los activos de la información hasta niveles aceptables, para esto se parte de la situación actual de la organización la cual permite definir el contexto y centrar los esfuerzos en los riesgos más relevantes.

Objetivo. Identificar los riesgos y amenazas para los activos de la información de la empresa RANDOM S.A.

Alcance. El análisis de riesgos se realiza para los procedimientos y activos de la información de la organización, enfocándose en los procesos tecnológicos que intervienen en el desarrollo de las operaciones del departamento de tecnologías de la información y cumplimiento de los objetivos misionales y del negocio. En el Cuadro 14 se registra el alcance del análisis de riesgos para la empresa RANDOM S.A.

Cuadro 14. Alcance del análisis de riesgos en la empresa RANDOM S.A.

Objetivo	Realizar la identificación, análisis y evaluación de los activos y riesgos de seguridad de la información del departamento TI.
Alcance	Análisis de riesgos para los procesos y procedimientos del departamento de Tecnología de la Información de la empresa RANDOM S.A.
Nombre de la Empresa	**RANDOM S.A.**
Normatividad	NTC ISO/IEC 27001
Enfoque metodológico	El enfoque de gestión de riesgos a aplicar está basado en la metodología **MAGERIT**.
Tratamiento	Se tratarán los riesgos cuyos niveles sean: **Nivel a tratar**
	16 a 26 INACEPTABLE(I)
	Se aceptarán los riesgos cuyos niveles sean: **Nivel a aceptar**
	10 a 15 MODERADO (A)
	Niveles de aceptación del riesgo (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I))
	Una vez aplicados los controles se acepta un riesgo de residual en niveles **APRECIABLE** o **IMPORTANTE**
	Criticidad residual (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico(C))
Fuente: El autor	

Para la estimación del riesgo, se propone un mapa de calor que permite localizar los riesgos que requieren de atención oportuna y prioritaria con respecto a otros activos de la información; de este modo se puede identificar el estado actual de la seguridad de la información en la empresa.

En el caso de estudio se enfocan los esfuerzos en los riesgos con nivel (I) Inaceptable, ponderación entre 16 a 26, y una vez se hayan aplicados los controles pertinentes, el nivel del riesgo residual a aceptar es (A) Apreciable, ponderación entre 10 a 15.

• **Contexto legal.** De acuerdo con lo definido en la matriz de cumplimiento normativo expedida por el MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones), se establecen las regulaciones legales que rigen la actividad empresarial, teniendo en cuenta la política fiscal, regulaciones laborales y del mercado, aspectos financieros y contractuales y de protección de datos personales y el segmento político referido a la autoridad política de los negocios.

• **Enfoque metodológico.** Para el análisis y gestión de riesgo se utiliza la metodología MAGERIT, donde se establecen diferentes etapas de recopilación de información cuantitativa y cualitativa con el objetivo de tener una visión global de los activos, vulnerabilidades y amenazas presentes en la organización o la dependencia a auditar, con esto se puede realizar la valoración de los riesgos de manera exacta y proponer los controles adecuados para tratar el riesgo, acorde con el alcance y directrices dadas por la gerencia. En cuanto al Plan Estratégico de Seguridad Informática, se toma como insumo los riesgos críticos que se identificaron y se propone el catálogo de proyectos en función de los dominios de la norma ISO 27001.

• **Identificación de los activos de información**. Para el caso estudio de la empresa RANDOM S.A, en el Cuadro 15 se presenta el listado de los activos más importantes que fueron identificados y su correspondiente descripción reconociendo la función que cumplen en la organización.

Cuadro 15. Identificación de los activos de información

Activo	Descripción	Ubicación	Cantidad
Servidores de Dominio	Servidor encargado de la autenticación para garantizar o denegar a un usuario el acceso a recursos de la red.	Centro de datos	2
Servidor de impresión	Servidor encargado de gestionar las impresiones en la organización.	Centro de datos	1
Servidor de Archivos	Servidor encargado de la gestión de archivos en la organización	Centro de datos	1
Equipos de protección eléctrica	UPS encargada de mantener fluido el centro de datos	Centro de datos	1
Centro de datos	Sitio donde se consolida los servicios de: Servidor de impresión, dominio, File server. El Centro de Cableado incluye: - Sistemas de detección de incendios. - Aire Acondicionado. - Control de acceso físico. - Extintores. - Equipos de protección eléctrica.	Edificio RANDOM S.A	1

Cuadro 15. (Continuación)

Activo	Descripción	Ubicación	Cantidad
ERP	Sistema que planifica todos los recursos empresariales de RANDOM S.A	Nube	1
SalesForce	Aplicativo CRM que gestiona toda la relación comercial de la organización.	Nube	1
Correo electrónico	Servicio de Office 365	Nube	1
Telefonía IP	Plantas telefónicas de todas las sedes. Teléfonos IP	Centro de Datos Oficinas	1 48
Equipos de cómputo de los usuarios finales Desarrollo de negocios	PC Sistema Operativo Windows 10 Laptop Sistema Operativo Windows 10	Oficina Desarrollo de negocios	5 7
Equipos de cómputo de los usuarios finales TI	PC Sistema Operativo Windows 10 Laptop Sistema Operativo Windows 10	Oficina de T.I	8 19
Equipos de cómputo de los usuarios finales Administrativo	PC Sistema Operativo Windows 10 Laptop Sistema Operativo Windows 10	Oficina de Administrativo	10 9
Fortigate 60D	Firewall perimetral que sirve para proteger las redes empresariales de ataques, spam, y otros peligros informáticos. Utilizado para gestión de servicios contratados por clientes.	Centro de Datos	4
Fortigate 100E	Firewall perimetral que sirve para proteger las redes empresariales de ataques, spam, y otros peligros informáticos. Utilizado para gestión de servicios contratados por clientes.	Centro de Datos	4
FortiAP 24D	Access Point que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica segura.	Distribuido en oficina y clientes	16
Fortigate 80E	Firewall perimetral que sirve para proteger las redes empresariales de ataques, spam, y otros peligros informáticos.	Centro de Datos	1
Cisco catalyst 9300	Dispositivos de red encargados de la interconexión de la red de datos	Centro de datos	3
Operadores NOC	Personal encargado de la gestión de servicios de networking	Oficina RANDOM S.A.	8

Cuadro 15. (Continuación)

Activo	Descripción	Ubicación	Cantidad
PRTG Network Monitor	PRTG Network Monitor es un software de monitoreo de red sin agentes de Paessler AG.	Centro de Datos	1
Contratos de servicio	Contratos con clientes que disfrutan de los servicios brindados por RANDOM.	Oficina RANDOM S.A.	13
Fuente: Enunciado del enfoque administrativo, curso de proyecto de seguridad informática II.			

- **Identificación de riesgos en los activos de información.** El listado de activos es el insumo para identificar las amenazas que pueden generar un impacto negativo y degradar al activo. En el Cuadro 16 se identifica cada amenaza clasificada según su naturaleza y asociada a una vulnerabilidad que puede ser aprovechada por un atacante informático.

Cuadro 16. Amenazas y vulnerabilidades asociadas a los activos

ID	Activo	Riesgo	Amenaza	Vulnerabilidad
RA1	Información	Critico	[E7] Deficiencias en la organización	La organización no cuenta con un sistema de gestión de seguridad de la información.
RA2	Servidores de Dominio	Critico	[E21] Errores de mantenimiento / actualización de programas (software)	No se cuenta con una política para ejecutar actualizaciones en horario no hábil, una actualización no programada en el servidor genera indisponibilidad en el servicio.
RA3	Servidor de impresión	Importante	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Al sistema no se le ha realizado mantenimiento periódico y puede fallar de manera súbita.
RA4	Servidor de Archivos	Critico	[I10] Degradación de los soportes de almacenamiento de la información	No se cuenta con un dispositivo de almacenamiento auxiliar en caso de falla del dispositivo principal.
RA5	Servidores y Estaciones de trabajo	Critico	[E14] Escapes de información	Ex filtración de información y fuga de datos sensibles para la organización.
RA6	Servidores y activos críticos de la organización	Critico	[A26] Ataque destructivo	Un activo critico tiene una vulnerabilidad que es aprovechada por un atacante y compromete la confidencialidad, integridad y disponibilidad de la información.

Cuadro 16. (Continuación)

ID	Activo	Riesgo	Amenaza	Vulnerabilidad
RA7	Equipos de protección eléctrica	Apreciable	[I7] Condiciones inadecuadas de temperatura o humedad	El activo se encuentra en un espacio donde no se cumplen condiciones de climatización óptimas.
RA8	Centro de datos	Importante	[N1] Fuego	No se cuenta con extintores especializados para equipos electrónicos.
RA9	ERP	Importante	[E14] Escapes de información	Cualquier colaborador puede autenticarse con las credenciales de dominio en el aplicativo ERP y no existen privilegios de acceso.
RA10	SalesForce	Critico	[A5] Suplantación de la identidad del usuario	El aplicativo no cuenta con segundo factor de autenticación y existen cuentas activas de usuarios que ya no laboran.
RA11	Correo electrónico	Critico	[E4] Errores de configuración	Error de configuración en el cliente de correo electrónico, no permite actualizar la bandeja de entrada.
RA12	Telefonía IP	Apreciable	[E25] Pérdida de equipos	El equipo no se cuenta asegurado a la estación de trabajo y puede ser sustraído de la organización.
RA13	Equipos de cómputo – Desarrollo de negocios	Importante	[A11] Acceso no autorizado	Un usuario deja desatentado la estación de trabajo y cualquier persona que tenga acceso físico al equipo, puede visualizar la información almacenada.
RA14	Equipos de cómputo – TI	Apreciable	[A22] Manipulación de programas	Se observan herramientas no autorizadas dentro de la línea base de la organización.
RA15	Equipos de cómputo – Administrativo	Importante	[A18] Destrucción de información	Los computadores portátiles no cuenta con cifrado en disco duro.
RA16	Fortigate 60 D	Importante	[A12] Análisis de tráfico	No existen controles de seguridad para actividades de reconocimiento e interceptación de paquetes.
RA17	Fortigate 100 E	Importante	[A24] Denegación de servicio	La segmentación de la RED no se ha documentado por lo cual cada vez que hay un inconveniente se debe invertir mucho tiempo.

Cuadro 16. (Continuación)

ID	Activo	Riesgo	Amenaza	Vulnerabilidad
RA18	FortiAP 24d	Importante	[I8] Fallo de servicios de comunicaciones	Los equipos operan en diferentes frecuencias y canales, por lo tanto se presenta interferencia.
RA19	Fortigate 80E	Critico	[A4] Manipulación de la configuración	Los Fortigates internos de la compañía no tienen reglas definidas ni licencia de uso.
RA20	Cisco catalyst 9300	Importante	[A23] Manipulación de los equipos	El equipo no tiene configurado credenciales de acceso y usa las credenciales de fábrica., generando que un atacante modifique la configuración.
RA21	Operadores NOC	Apreciable	[A28] Indisponibilidad del personal	Por motivos de manifestaciones y desmanes de orden público, el personal no puede desplazarse hasta la sede de la empresa.
RA22	PRTG Network Monitor	Importante	[E20] Vulnerabilidades de los programas (software)	La versión instalada esta desactualizada y se ha descubierto un CVE para obtener la base de datos de usuarios.
RA23	Contratos de servicio	Importante	[E18] Destrucción de información	Los contratos son almacenados en un área común y cualquier empleado tiene acceso.
RA24	Normatividad legal vigente en protección de datos	Critico	[E7] Deficiencias en la organización	No se cumple con los requerimientos de la ley de protección de datos - 1581 de 2012.

Fuente: El autor, basado en la metodología MAGERIT, libro III – Técnicas

- **Análisis y valoración de los riesgos.** Con base en el ítem anterior, se procede a clasificar los activos e identificar el riesgo estableciendo un indicador cuantitativo para cada uno de los pilares de la seguridad de la información, donde:

  - **A:** Autenticidad
  - **T:** Trazabilidad
  - **C:** Confidencialidad
  - **I:** Integridad
  - **D:** Disponibilidad

Para la valoración cuantitativa se tiene definida la siguiente escala de valor:

- Crítico: 21 a 25 – (Muy alto).
- Importante: 16 a 20 - (Alto).
- Apreciable: 10 a 15 – (Medio).
- Bajo: 5 a 9 - (Bajo).
- Despreciable: 1 a 4 – (Muy bajo).

Para obtener la valoración del riesgo, es necesario realizar el producto entre la probabilidad de presentarse un evento adverso y el impacto que se genera sobre un activo de la información. En el Cuadro 17 se registra la valoración del riesgo para cada uno de los activos identificados, clasificándolos según las categorías expuestas por MAGERIT y contrastando cada riesgo con las propiedades de la información.

Cuadro 17. Valoración del riesgo

ID	Activo	Clasificación	A	T	C	I	D	Riesgo
RA1	Información	[D] Datos	25	20	20	20	25	Critico
RA1	Servidores de Dominio	[HW] Equipamiento informático	25	20	20	20	25	Critico
RA2	Servidor de impresión	[HW] Equipamiento informático	15	20	15	15	15	Importante
RA3	Servidor de Archivos	[HW] Equipamiento informático	20	15	25	25	20	Critico
RA5	Servidores y Estaciones de trabajo	[HW] Equipamiento informático	20	15	25	25	20	Critico
RA6	Servidores y activos críticos de la organización	[HW] Equipamiento informático	20	15	25	25	20	Critico
RA4	Equipos de protección eléctrica.	[AUX] Equipamiento auxiliar	4	4	15	15	20	Apreciable
RA5	Centro de datos	[L] Instalaciones	20	4	20	15	25	Importante
RA6	ERP	[SW] Software	20	15	25	20	20	Importante
RA7	SalesForce	[SW] Software	20	15	25	20	25	Critico
RA8	Correo electrónico	[SW] Software	20	20	25	25	20	Critico
RA9	Telefonía IP	[AUX] Equipamiento auxiliar	9	15	15	15	15	Apreciable
RA10	Equipos de cómputo de los usuarios finales –	[HW] Equipamiento informático	20	20	15	15	20	Importante

Cuadro 17. (Continuación)

ID	Activo	Clasificación	A	T	C	I	D	Riesgo
RA11	Equipos de cómputo de los usuarios finales – TI	[HW] Equipamiento informático	20	9	15	15	15	Apreciable
RA12	Equipos de cómputo de los usuarios finales – Administrativo	[HW] Equipamiento informático	20	20	15	15	20	Importante
RA13	Fortigate 60 D	[COM] Redes de comunicaciones	20	15	20	20	25	Importante
RA14	Fortigate 100 E	[COM] Redes de comunicaciones	20	15	20	20	25	Importante
RA15	FortiAP 24d	[AUX] Equipamiento auxiliar	20	15	15	15	15	Importante
RA16	Fortigate 80E	[COM] Redes de comunicaciones	20	15	20	20	25	Importante
RA17	Cisco catalyst 9300	[COM] Redes de comunicaciones	20	15	20	20	25	Importante
RA18	Operadores NOC	[P] Personal	20	15	15	0	20	Apreciable
RA19	PRTG Network Monitor	[SW] Software	20	20	15	15	20	Importante
RA20	Contratos de servicio	[MEDIA] Soporte de información	20	20	15	15	20	Importante
RA24	Normatividad legal vigente en protección de datos	[MEDIA] Soporte de información	20	15	25	25	20	Critico

Fuente: El autor, basado en la metodología MAGERIT, libro III – Técnicas

La valoración del riesgo es realizada a partir de la clasificación de activos y la caracterización de amenazas; está en función de los pilares de la seguridad de la información y se mide mediante los parámetros de magnitud de la posible pérdida de un activo y la probabilidad de que el daño pueda ocurrir. La valoración de riesgos permite saber en que invertir los recursos y como administrar los esfuerzos para el tratamiento de los riesgos críticos, importantes, moderado y bajos, respectivamente

El mapa de calor establece el nivel del manejo y tiempo de respuesta, debido a que todos los activos son importantes y es necesario protegerlos, pero deben tener prioridad los activos críticos con un nivel de tratamiento urgente. A modo general y basado en las etapas anteriores, en la Cuadro 18 se define el mapa de calor que permite ubicar los riesgos según su valoración.

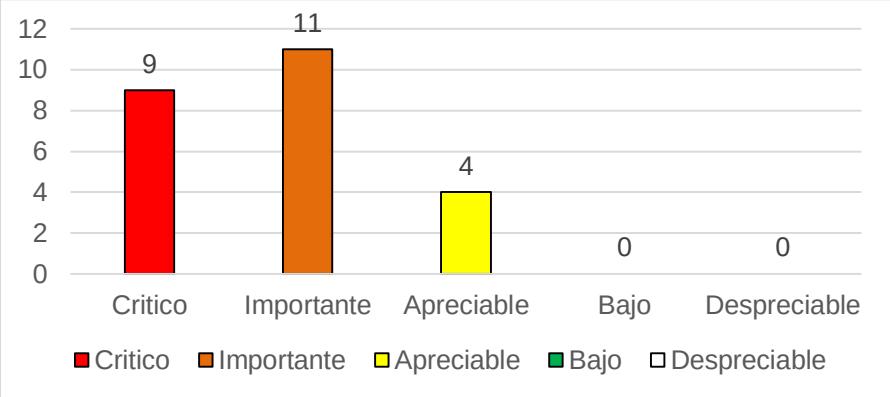
Cuadro 18. Mapa de calor para la gestión del riesgo

IMPACTO						
	MA					RA1 - RA2 - RA4 - RA5 - RA6 - RA10 - RA11 - RA19 - RA24
	A				RA3 - RA8 - RA9 - RA13 - RA15 - RA16	RA17 - RA18 - RA20 - RA22 - RA23
	M				RA7 - RA12 - RA14 - RA21	
	B					
	MB					
	RIESGO	MB	B	M	A	MA
		PROBABILIDAD				

El autor, basado en la metodología MAGERIT, libro III – Técnicas

En la Figura 143 se presenta la gráfica sobre la clasificación de severidad; se logró identificar que 9 riesgos tienen un nivel crítico y requieren ser abordados inmediatamente porque sus amenazas son las que mayor posibilidad tienen de materializarse.

Figura 143. Severidad de los riesgos identificados



Fuente: El autor

• **Propuesta para el tratamiento del riesgo**. Es la fase final donde se comprende que acciones se deben tomar ante los riesgos más importantes que se identificaron previamente y cuáles serán las medidas para su adecuado manejo. Este es un proceso clave durante una auditoria porque no tendría relevancia que se identificaran y valoraran activos en etapas anteriores si no se pretende asumir y aplicar las medidas pertinentes ante los hallazgos encontrados.

La gestión de riesgos cuenta con un enfoque evolutivo, dinámico y continuo, por lo tanto, es importante resaltar que los riesgos presentan diferentes tipos de características y nivel de importancia, por eso es necesario clasificarlos, priorizarlos, evaluarlos y tratarlos de la mejor manera que sea posible; en el Cuadro 19 se presenta las diferentes acciones para el tratamiento del riesgo en la empresa Random S.A.

Cuadro 19. Tratamiento del riesgo

ID	Activo	Riesgo	Tratamiento	Control
RA1	Información	Critico	Transferir	Contratar servicios de consultoría y asesoramiento para la implementación del SGSI.
RA2	Servidores de Dominio	Critico	Mitigar	Desarrollar el procedimiento de actualizaciones periódicas para los activos críticos de la organización.
RA4	Servidor de Archivos	Critico	Mitigar	Adquirir un dispositivo de almacenamiento de respaldo e implementarlo en el servidor de archivos.
RA5	Servidores y Estaciones de trabajo	Critico	Mitigar	Implementar la política de prevención de perdida de datos a nivel de *endpoint* en los servidores y estaciones de trabajo.

Cuadro 19. (Continuación)

ID	Activo	Riesgo	Tratamiento	Control
RA6	Servidores y activos críticos de la organización	Critico	Mitigar	Desarrollar el procedimiento de gestión de vulnerabilidades, a fin de evaluar brechas y debilidades en activos y aplicaciones críticas.
RA10	SalesForce	Critico	Mitigar	Configurar doble factor de autenticación vía SMS sobre todas las cuentas activas y deshabilitar las cuentas inactivas.
RA11	Correo electrónico	Critico	Mitigar	Establecer el procedimiento de configuración para los clientes de correo electrónico en estaciones de trabajo y móviles.
RA19	Fortigate 80E	Critico	Mitigar	Realizar un estudio del tráfico de la red y generar las políticas correspondientes, según el perfil del usuario. Adquirir el licenciamiento con el fabricante.
RA24	Normatividad legal vigente en protección de datos	Critico	Transferir	Contratar servicios de consultoría y asesoramiento para la implementación de medidas de cumplimiento de la ley 1581 de 2012.
RA3	Servidor de impresión	Importante	Transferir	Contratar servicios profesionales para realizar el mantenimiento preventivo para los servidores y activos críticos.
RA8	Centro de datos	Importante	Mitigar	Adquirir extintores tipo A, B, C, D y K, los cuales deben ser ubicados estratégicamente en las áreas adecuadas.
RA9	ERP	Importante	Mitigar	A nivel de desarrollo se deben definir privilegios de acceso y establecer los perfiles que deben tener acceso a la herramienta ERP, otorgando permisos por rol.
RA13	Equipos de cómputo de los usuarios finales – Desarrollo de negocios	Importante	Mitigar	Definir la política de equipo desatendido, además, se debe aplicar la directiva de bloqueo por tiempo de inactividad a nivel de directorio activo.
RA15	Equipos de cómputo de los usuarios finales – Administrativo	Importante	Mitigar	Establecer el procedimiento de cifrado de discos para que el departamento de tecnología lo aplique en todas las estaciones de trabajo.

Cuadro 19. (Continuación)

ID	Activo	Riesgo	Tratamiento	Control
RA16	Fortigate 60 D	Importante	Transferir	Adquirir servicios profesionales de monitoreo y correlación de eventos de seguridad SIEM.
RA17	Fortigate 100 E	Importante	Mitigar	Realizar la segmentación de la red acorde con la cantidad de usuarios, este proceso debe quedar documentado.
RA18	FortiAP 24d	Importante	Aceptar	Se contempla cambiar el modo de operación de los Access Point al canal 11 de 2,4 Ghz, pero temporalmente se continua operando en el canal 6.
RA20	Cisco catalyst 9300	Importante	Mitigar	Se debe aplicar hardening en la configuración de acceso basado en recomendaciones hechas por el fabricante.
RA22	PRTG Network Monitor	Importante	Mitigar	Realizar el plan de trabajo para aplicar la actualización sobre la plataforma de monitoreo de seguridad.
RA23	Contratos de servicio	Importante	Mitigar	Realizar la digitalización de los contratos físicos y proceder con el almacenamiento seguro en un área restringida.
RA7	Equipos de protección eléctrica.	Apreciable	Aceptar	Mientras se adecua un sitio adecuado y seguro, los equipos de protección eléctrica deben permanecer en el lugar actual.
RA12	Telefonía IP	Apreciable	Aceptar	Cada funcionario es responsable del equipamiento informático asignado para desarrollar sus funciones.
RA14	Equipos de cómputo de los usuarios finales – TI	Apreciable	Mitigar	El personal de soporte técnico se encarga de realizar revisiones periódicas a los programas y características instalados en los sistemas operativos.
RA21	Operadores NOC	Apreciable	Aceptar	Se cuenta con la estrategia de sitio alterno para que los colaboradores realicen sus actividades de manera remota usando VPN.

Fuente: El autor, basado en la metodología MAGERIT, libro III – Técnicas

6.3.2 Proyectos de seguridad Informática. Con base en los diferentes riesgos identificados, es necesario definir los proyectos que mitigan el impacto asociado y definir la correspondiente prioridad acorde con su nivel de relevancia para la organización. Los proyectos de seguridad informática para fortalecer la estrategia de ciberseguridad en la organización son desarrollados por el comité de seguridad informática, el departamento de tecnologías de la información y el área de seguridad informática. En el Cuadro 20 se realiza la justificación de la situación actual y deseada para cada uno de los proyectos de seguridad informática relevantes.

Cuadro 20. Modelo *AS – TO BE* de RANDOM S.A.

Aspecto de seguridad	Situación actual (AS IS)	Situación deseada (TO BE)
Sistema de Gestión de Seguridad de la Información - SGSI	RANDOM S.A. no cuenta con un Sistema de Gestión de Seguridad de la información	Implementar el sistema de gestión de seguridad de la información.
Acceso a la información	Los colaboradores pueden acceder a cualquier repositorio de la organización y no se requiere credenciales de acceso.	Habilitar el cifrado de unidades de almacenamiento en las estaciones de trabajo de la organización.
Transferencia Segura de Información	No existe un procedimiento para la transferencia segura de información.	Establecer las medidas necesarias para garantizar la seguridad durante la transferencia de información.
Seguridad perimetral	La segmentación de la RED no se ha documentado por lo cual cada vez que hay un inconveniente se debe invertir mucho tiempo. Los Fortigates internos de la compañía no tienen reglas definidas ni licencia de uso.	Aplicar reglas de navegación y perfiles de seguridad de acuerdo con el cargo del colaborador. Documentar las reglas de navegación. Adquirir el licenciamiento con el fabricante.
Monitoreo de eventos de seguridad	No se cuenta con una herramienta SIEM para la trazabilidad de eventos de auditoria, red, sistema y aplicación.	Adquirir el servicio de correlación de eventos para detectar en tiempo real amenazas hacia los activos de la información.
DLP (Data Loss Protection)	No se tiene una herramienta que cumpla la función de prevención de perdida de datos. En los últimos 2 años se han generados perdida de datos debido a empleados inconformes.	Implementar una solución para la prevención de perdida de datos. Desarrollar casos de uso sobre perdida de datos, para que sean alertados de manera oportuna
Gestión de Vulnerabilidades	No se ha realizado un escaneo de vulnerabilidades a los activos críticos.	Elaborar el procedimiento de gestión de vulnerabilidades y definir el tratamiento adecuado

Cuadro 20. (Continuación)

Aspecto de seguridad	Situación actual (AS IS)	Situación deseada (TO BE)
Continuidad del negocio	No se cuenta con un análisis de impacto del negocio y tampoco se cuenta con el plan de recuperación ante desastres.	Elaborar el documento de análisis de impacto del negocio y realizar la documentación para el plan de recuperación de desastres.
Sensibilización en seguridad de la información	Se realizan charlas sobre seguridad de la información cada 6 meses.	Implementar el plan de sensibilización y capacitación de seguridad de la información.
Hacking ético	No se tiene definido el proceso de pruebas de penetración.	Adquirir un servicio de *pentesting* que se ejecute cada 6 meses.
Protección de datos personales	La organización no cumple con los requerimientos de seguridad de la Ley 1581 de 2012 de protección de datos personales.	Implementar las medidas para cumplir los requerimientos de la ley 1581 de 2012.
Fuente: El autor		

6.3.2.1 Sistema de Gestión de Seguridad de la Información – SGSI. Implementar un sistema de gestión de seguridad de la información, el cual sirva de apoyo para garantizar los pilares de seguridad de la información para todos los procesos que utilicen datos críticos de la organización. Proteger la información de diferentes amenazas, vulnerabilidades y riesgos asociados a los activos de la información**.**

Actividades: En el ciclo de mejora continua se proponen las siguientes etapas de implementación de un SGSI:

- Planificar: Establecer el alcance del SGSI, definir políticas se seguridad, indicar la declaración de aplicabilidad y realizar el análisis de riesgos.
- Hacer: Implementar controles, definir el plan de tratamiento del riesgo, definir las métricas de ciberseguridad y contratar servicios de monitoreo de seguridad.
- Verificar: Evaluar la efectividad del SGSI, verificar los controles y planes de seguridad, además de llevar a cabo las auditorias correspondientes.
- Actuar: Realizar mejoras identificadas, sensibilizar al personal operativo y continuar con el ciclo de mejora continua.

Dominio ISO 27001: Aplica para todos los dominios de la norma ISO 27001.

Complejidad: Alta.

6.3.2.2 DLP (Data Loss Protection). Las herramientas de prevención de perdida de datos permiten evitar la trasferencia no autorizada de información confidencial afuera de la red por parte de colaboradores de la organización.

Actividades: Implementar una herramienta o integrar un módulo DLP en la solución de antivirus *Endpoint* de la organización.
Dominio ISO 27001: Aplica para el dominio de control A12. Seguridad en las operaciones.
Complejidad: Baja.

6.3.2.3 Acceso a la información. Desarrollar una política para el control de acceso a la información importante de la organización, para garantizar el ingreso seguro a los datos se establece el procedimiento de control de acceso con sus respectivos controles.

Actividades: Se requiere definir una política de control de acceso, donde se establezcan procedimientos tales como el acceso a los servicios de la red, permisos, privilegios, gestión de contraseñas, ingreso o restricción de acceso a la información. Implementar los controles, técnicas y medidas asociadas al control de acceso.
Dominio ISO 27001: Aplica para el dominio de control A9. Control de accesos.
Complejidad: Media.

6.3.2.4 Transferencia Segura de Información. Desarrollar una política para transferencia segura de la información importante de la organización, para garantizar la transmisión segura de los datos se establece el procedimiento de trasferencia segura con sus respectivos controles.

Actividades: Implementar las medidas técnicas para garantizar la transferencia segura de la información sobre la infraestructura tecnológica de la organización. Implementar los controles y medidas como seguridad en los servicios de red o control y segregación de redes.
Dominio ISO 27001: Aplica para el dominio de control A13. Seguridad en las telecomunicaciones.
Complejidad: Media.

6.3.2.5 Seguridad perimetral. Es necesario segmentar las redes internas de la organización para las áreas descritas en el organigrama, con base en esto, se aplican los perfiles de navegación según el departamento al cual pertenece el colaborador y los permisos otorgados por el coordinador del área. Del mismo modo se aplica una filosofía negativa, donde se deniega todo el tráfico al inicio y se permite únicamente lo explícito.

Actividades: Se debe evaluar el tráfico de la red y verificar que usuarios acceden a que recursos, con base en este estudio se deben aplicar las reglas y perfiles de seguridad corresponde a las áreas. Después de aplicar las reglas, deben ser documentadas completamente para futuras ocasiones donde se requiera validar el comportamiento de la red.

Dominio ISO 27001: Aplica para el dominio de control A13. Seguridad en las telecomunicaciones.
Complejidad: Media.

6.3.2.6 Monitoreo de eventos de seguridad. El monitoreo de eventos de seguridad permite predecir solicitudes maliciosas que atentan contra los activos de información de la organización, por lo tanto, las herramientas de correlación de eventos de seguridad ofrecen visibilidad en tiempo real.

Actividades: Se requiere contratar un servicio de monitoreo de ciberseguridad con un proveedor externo para tener alertas de seguridad sobre la infraestructura tecnológica de la organización. Para esto, se debe establecer una VPN sitio a sitio, entre la organización y el proveedor externo, para enviar de manera segura la información.
Dominio ISO 27001: Aplica para el dominio de control A16. Gestión de incidentes de seguridad.
Complejidad: Media.

6.3.2.7 Gestión de Vulnerabilidades. Es un proceso continuo en el cual se realiza una serie de pruebas técnicas para detectar posibles brechas de seguridad en los activos de la información críticos en la organización. El orden de prelación define que los activos con mayor criticidad son los sistemas centrales, servidores, aplicaciones internas y las estaciones de trabajo.

Actividades: Aplicar el ciclo de gestión de vulnerabilidades para los activos de información más importantes para la organización. El ciclo está compuesto por las etapas de inventario de activos, planeación, ejecución, reporte, identificación de amenazas, remediación y validación.
Dominio ISO 27001: Aplica para el dominio de control A12. Seguridad en las operaciones.
Complejidad: Alta.

6.3.2.8 Continuidad del negocio. El plan de continuidad de negocio permite mantener la operación durante una situación adversa con la finalidad de disminuir el impacto del cese de actividades en la organización. Esto se ve reflejado en la gestión de la capacidad y como se asignan los recursos para continuar prestando los servicios críticos.

Actividades: Desarrollar el análisis de impacto del negocio, análisis de riesgos, definición de estrategias de continuidad, desarrollar el plan de recuperación ante desastres, evaluar y mantener el plan de continuidad.
Dominio ISO 27001: Aplica para el dominio de control A17. Continuidad del negocio
Complejidad: Alta.

6.3.2.9 Sensibilización en seguridad de la información. La concienciación y la capacitación de competencias digitales y de protección de la información, son un componente esencial para formar a los colaboradores y enseñarles a detectar una amenaza en tiempo real, además también genera sentido de pertenecía con el uso y manejo que se le da a la información de la organización.

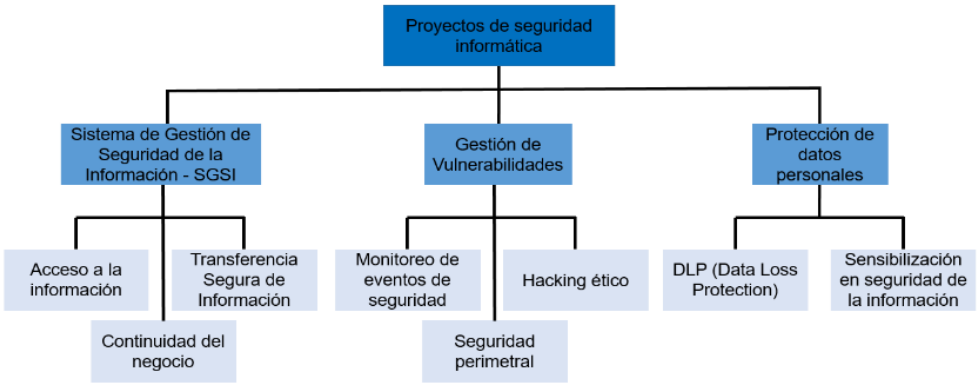
Actividades: Realizar un procedimiento donde se indiquen las campañas de sensibilización en seguridad informática y la periodicidad en las que se deben llevar a cabo. Tales campañas pueden ser capacitación, charlas, medios audiovisuales, entre otros.
Dominio ISO 27001: Aplica para el dominio de control A7. Seguridad en los recursos humanos.
Complejidad: Media.

6.3.2.10 Protección de datos personales. El cumplimiento de la ley de datos personales permite garantizar el correcto tratamiento de información personal de colaboradores, proveedores y clientes que es almacenada en bases de datos o archivos de la organización.

Actividades: Establecer el procedimiento donde se especifique las medidas y controles para el manejo, recolección y almacenamiento de datos personales para garantizar el cumplimiento de la ley 1581 de 2012.
Dominio ISO 27001: Aplica para el dominio de control A18. Cumplimiento.
Complejidad: Alta.

En la Figura 144 se encuentra la organización jerárquica de los proyectos de seguridad informática según su línea de impacto.

Figura 144. Estructura del PESI



Fuente: El autor

6.3.2.11 Cronograma de los proyectos de seguridad. La definición del cronograma de ejecución de proyectos está planteada para los próximos 3 años, es decir 2020 – 2022 y se encuentra registrado en el Cuadro 21.

Cuadro 21. Cronograma de los proyectos de seguridad

Proyecto de seguridad	2020	2021	2022
SGSI	Diseñar e implementar el SGSI en la organización	Proceso de auditoría del SGSI.	Certificación del SGSI.
Acceso a la información	Asignación de permisos y privilegios.	Gestión de identidades.	-
Transferencia segura de información	Implementar técnicas de cifrado.	Implementación de VPN.	-
Seguridad perimetral	Creación de reglas. Adquisición de licenciamiento.	Documentación de reglas.	-
Monitoreo de eventos de seguridad	Adquirir servicios de SOC operaciones en seguridad.	Modelamiento de casos de uso.	Renovar servicios de SOC operaciones en seguridad.
DLP (Data Loss Protection)	Adquirir un módulo de DLP sobre la solución de antivirus.	Notificaciones sobre ex filtración de datos.	Perfiles de seguridad DLP en el UTM.
Gestion de vulnerabilidades	Adquirir servicios de gestión de vulnerabilidades. Realizar escaneo de vulnerabilidades.	Realizar escaneo y remediación de vulnerabilidades.	Realizar escaneo y remediación de vulnerabilidades.
Continuidad del negocio	Elaboración y diseño del BIA y DRP.	Implementación del DRP	Auditoria del DRP.
Sensibilización	Diseñar el plan de capacitación. Realizar campañas de sensibilización y cursos de ciberseguridad.	Realizar campañas de sensibilización y cursos de ciberseguridad.	Realizar campañas de sensibilización y cursos de ciberseguridad.
Hacking ético	Adquirir servicios de *pentesting*. Realizar pruebas de seguridad cada 6 meses.	Realizar pruebas de seguridad cada 6 meses	Realizar pruebas de seguridad cada 6 meses
Protección de datos personales	Diseñar la política de protección de datos personales.	Implementar las medidas pertinentes para el manejo de datos personales.	Evaluar las medias y el manejo de datos personales.

Fuente: El autor

6.3.2.12 Inversión económica de cada proyecto de seguridad. La estimación de la inversión económica de cada proyecto está en función de la moneda local colombiana; se encuentra dividida por etapas de implementación para cada proyecto y según el periodo establecido para el PESI, lo anterior se encuentra incluido en el Cuadro 22.

Cuadro 22. Inversión económica de cada proyecto de seguridad

Proyecto de seguridad	**Fase I 2020**	**Fase II 2021**	**Fase III 2022**	**Total**
SGSI	25.000.000	5.000.000	5.000.000	40.000.000 COP
Acceso a la información	10.000.000	5.000.000	-	15.000.000 COP
Transferencia segura de información	15.000.000	5.000.000	-	20.000.000 COP
Seguridad perimetral	55.000.000	5.000.000	-	60.000.000 COP
Monitoreo de eventos de seguridad	30.000.000	30.000.000	20.000.000	80.000.000 COP
DLP (Data Loss Protection)	5.000.000	5.000.000	5.000.000	15.000.000 COP
Vulnerabilidades	20.000.000	5.000.000	5.000.000	30.000.000 COP
Continuidad del negocio	5.000.000	15.000.000	5.000.000	25.000.000 COP
Sensibilización	10.000.000	5.000.000	5.000.000	20.000.000 COP
Hacking ético	15.000.000	10.000.000	10.000.000	35.000.000 COP
Protección de datos personales	5.000.000	5.000.000	5.000.000	15.000.000 COP
Total	**195.000.000**	**95.000.0000**	**60.000.000**	**355.000.000 COP**

Fuente: El autor

7. CONCLUSIONES

Al culminar el presente proyecto aplicado sobre virtualización de sistemas operativos, uso de herramientas de *ethical hacking* para realizar ataques informáticos bajo un ambiente controlado y planeación estratégica de ciberseguridad, se puede concluir que el desarrollo del mismo ha contribuido para evaluar el estado de la seguridad de la información en la empresa RANDOM S.A.

- El principal objetivo de un análisis de riesgos es ofrecer de manera organizada, clara y documentada que activos relevantes requieren aseguramiento basado en su clasificación y las dimensiones de la información, la probabilidad en función del impacto si se materializa una amenaza, nivel de tratamiento y la relevancia. Las metodologías de análisis de riesgos son la fase inicial de cara a implementar un SGSI en una organización, de allí resalta su importancia dado que, si el análisis de riesgos ha cubierto todos los activos y sus posibles amenazas de extremo a extremo en la organización, la definición, implementación y automatización de controles será eficiente y apoyará los lineamentos de alto nivel establecidos en cualquier plan de la seguridad de la información.

- Luego de realizar la evaluación de vulnerabilidades sobre los servidores de la organización se identificaron brechas y debilidades en la configuración establecida para ambos servidores. Acorde con lo dicho previamente, en este documento se refleja el paso a paso detallado de cómo generar un ataque informático con base en las vulnerabilidades encontradas. Así mismo se establecen los procedimientos, políticas y controles pertinentes para prevenir este tipo de intrusiones, generando una mejora en el estado actual de la seguridad de los activos comprometidos por el ataque informático.

- La planeación estratégica de seguridad informática mejora el nivel de madurez y fortalece la postura de seguridad en las organizaciones, esto se produce gracias a la generación de proyectos e iniciativas en pro de la prevención y la protección de la información. Esta planeación de seguridad está acorde con las necesidades y requerimientos del negocio, alineándose con el gobierno corporativo y estándares reconocidos a nivel mundial.

- La seguridad informática cada día tiene un mayor impacto en las organizaciones, por lo tanto, es pertinente abordarla como un campo de aplicación que requiere de un alto grado de investigación teórica y aplicación práctica, convirtiéndola en un saber integral y completo. La planeación estratégica de ciberseguridad resuelve diferentes desafíos tecnológicos mediante la ejecución de proyectos que cumplen los diferentes objetivos de control de la norma ISO 27001.

8. RECOMENDACIONES

Después de realizar las pruebas correspondientes a los servidores comprometidos de la empresa RANDOM S.A, se pudo identificar que la principal vulnerabilidad estaba relacionada con fallas en la configuración y versiones obsoletas a nivel de aplicaciones y sistema operativo, conforme a esto, a continuación, se realizan una serie de recomendaciones que el departamento TI debe tener en cuenta para evitar posibles ataques informáticos.

- Realizar la actualización periódica del sistema operativo y de las aplicaciones instaladas en los servidores. Esta tarea debe realizarse dependiendo la criticidad del activo y las metas del negocio, además se recomienda su ejecución en un horario no hábil para no afectar la operación de la organización.

- Para equipos que van a cumplir la función de servidor en la red, es necesario instalar una versión de sistema operativo acorde con el rol que la maquina va a desempeñar en la red, además, se sugiere desactivar todos los servicios y protocolos que no se van a utilizar, esto incluye el bloqueo de sus correspondientes puertos desde el equipo perimetral. En los servidores se debe configurar el firewall integrado en cada una de las máquinas y mantenerlo activado para redes privadas y públicas.

- Para mitigar el impacto generado por las ciber-amenazas es necesario conocer su significado y modo de funcionamiento, además se evidencia que actualmente existen diferentes tipos de vectores de ataque que requieren ser plenamente detectados e identificados para su posterior manejo y/o tratamiento. Con base en esto se requiere establecer un plan periódico para realizar un análisis de vulnerabilidades y validar el estado actual de la configuración en los servidores.

- Establecer una política para realizar el respaldo periódico de los archivos y las configuraciones, de tal manera que se pueda restablecer en caso de un incidente sobre la máquina. Esta actividad se realiza semanalmente para los activos críticos de la organización y bajo demanda según solicitud previa de un usuario. Además, se recomienda realizar la depuración de los archivos innecesarios como temporales, informes de errores y cualquier otro tipo de información irrelevante que ocupe espacio en el disco duro de la máquina.

- El diseño e implementación de cualquier solución o herramienta de seguridad que involucre el mejoramiento de la seguridad de la información para una organización requiere de una fase previa de análisis y conocimientos teóricos sobre técnicas, buenas prácticas y estrategias para llevar a cabo un enfoque de seguridad en profundidad.

BIBLIOGRAFÍA

ACOSTA, Nubia & LEÓN, Tania. Diseño del Sistema de Gestión de Seguridad de la Información (S.G.S.I) para el centro de datos de la personería de Bogotá D.C. bajo las normas NTC-ISO-IEC 27001:2013 y GTC-ISO-IEC 27002:2013. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2017, [En línea]. (Recuperado en noviembre 2019.) Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11940/35508879.pdf

ACUARIO DEL PINO Santiago, Delitos informáticos: generalidades, [En línea]. (Recuperado en octubre 2018.) Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

ÁVILA GUALDRÓN, Miguel Andrés. Estudio de las mejores prácticas de ethical hacking, para generar un nuevo método que facilité la ejecución de análisis de seguridad enfocados a pruebas de penetración. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2018, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://repository.unad.edu.co/bitstream/10596/21293/4/1140816134.pdf

BYTE TI. La importancia y el riesgo del factor humano en la ciberseguridad. [En línea]. (Recuperado en octubre 2019.) Disponible en: https://www.revistabyte.es/publirreportaje/riesgo-factor-humano-la-ciberseguridad/.

CARAZO TORRES Omar. Elaboración de un Plan de Seguridad de la Información. [En línea]. (Recuperado en octubre 2019.) Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23004/6/ocarazotTFM0613memoria.pdf

CENTRO CIBERNÉTICO POLICIAL, Informe: Tendencias del cibercrimen en Colombia 2019 - 2020, [En línea]. (Recuperado en octubre 2020.) Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

CLARK Ben & WHITE. Alan. Blue Team Field Manual Version 1. Estados Unidos: Matt hulse, 2017. ISBN: 978-1541016361

CLARK Ben. Red Team Field Manual Version 1. a. Estados Unidos: Joe Vest, 2013. ISBN: 978-1494295509

COLOMBIA, ICONTEC. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC27001. [En Línea]. (Recuperado en noviembre 2019.) Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Ley 1273 de 2009, De la protección de la información y de los datos, [En línea]. (Recuperado en octubre 2018.) Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

COLOMBIA. MINISTERIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Lo que usted debe saber del CONPES de Seguridad Digital, [En línea]. (Recuperado en octubre 2018.) Disponible en: https://www.mintic.gov.co/portal/604/w3-article-15410.html

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Guía para la Implementación de Seguridad de la Información en una MIPYME, [En línea]. (Recuperado en octubre 2018.) Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

CORPOURABA. Plan estratégico de seguridad de la información 2018-2021. [En línea]. (Recuperado en octubre 2019.) Disponible en: http://corpouraba.gov.co/wp-content/uploads/Plan-Estrat%C3%A9gico-de-Seguridad-de-la-Informaci%C3%B3n-2019.pdf

CRUZ MORENO, Oscar Alonso. Diseño e implementación de un proceso de hardening. Tesis de Grado Ingeniería en Sistemas: Fundación Universitaria los Libertadores, 2018, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://repository.libertadores.edu.co/bitstream/handle/11371/1298/cruzoscar2017.pdf?sequence=3&isAllowed=y

CVE Common Vulnerabilities and Exposures, CVE® is a list of entries—each containing cybersecurity vulnerabilities. [En línea]. (Recuperado en diciembre 2018.) Disponible en: https://cve.mitre.org/

DE LOS SANTOS. Sergio. Una al día: Once años de seguridad informática. Madrid: Hispasec, 2009. ISBN: 978-1-4092-4380-9

DÍAZ RICARDO, Luis Carlos. Diseño de un Sistema de Gestión de la Seguridad de la Información en la IPS Aassalud de Corozal Sucre, mediante la implementación de la metodología Magerit (v3.0) y la Norma ISO 27001:2013. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2017, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/14386/1066172091.pdf

DORDOIGNE. José. Redes informáticas, nociones fundamentales 5° Edición, Virtualización de aplicaciones, 2015. ISBN: 978-2-7460-9733-9

ESPAÑA, MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I – Método, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://www.ccn-cert.cni.es/pdf/documentos-publicos/1789-magerit-libro-i-metodo/file.html

ESPAÑA, MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II - Catálogo de Elementos, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

ESPAÑA, MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro III - Guía de Técnicas, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

GARCÍA RAMBLA Juan Luis. Ataques en redes de datos IPv4 e IPv6. 2017. ISBN: 978-84-617-9278-8

GONZÁLEZ PÉREZ Pablo y ALONSO José María. Metasploit para Pentesters. 2017. ISBN: 978-84-617-1516-9

GUTIÉRREZ, D. M. & Pagés, A. C. Planificación y gestión de proyectos informáticos [En Línea]. [En línea]. (Recuperado en octubre 2019.) Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10280334&p00=pmi+pmbok+5

HERZOG Pete e ISECOM, OSSTMM 3 – The Open Source Security Testing Methodology Manual, [En línea]. (Recuperado en noviembre 2018.) Disponible en: http://www.isecom.org/mirror/OSSTMM.3.pdf

ICA. Instituto Colombiano Agropecuario. Plan estratégico de seguridad de información. [En línea]. (Recuperado en octubre 2019.) Disponible en: https://www.ica.gov.co/getattachment/Areas/Oficina-de-Tecnologias-de-la-Informacion/Plan-Estrategico-de-Seguridad-de-la-Informacion.pdf.aspx?lang=es-CO

INCIBE. Plan Director de Seguridad de la Información. [En línea]. (Recuperado en octubre 2019.) Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

INCIBE. Gestión de riesgos, Una guía de aproximación para el empresario. [En línea]. (Recuperado en noviembre 2019.) Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

LOZANO OLAVE M. Diseño de un plan estratégico de seguridad de información (pesi) para una compañía del sector asegurador [En línea]. (Recuperado en octubre 2019.) Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/1004/3.Documento%20final_Plan%20Estrategico%20de%20Seguridad%20de%20la%20Informaci%C3%B3n%20para%20una%20compa%C3%B1ia%20de%20seguros.pdf?sequence=1&isAllowed=y

MARÍN OSPINA, María Elena. Diseño e implementación de una política de seguridad de información, en el grupo de trabajo cuentas por pagar del ministerio de transporte. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2017, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://repository.unad.edu.co/bitstream/10596/14261/1/51820281.pdf

MUÑOZ, Jorge. Diseño de un plan estratégico para la seguridad de la información de Cias & Profesionales S.A.S [En línea]. (Recuperado en octubre 2019.) Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14448/1/80029231.pdf

NVT NATIONAL VULNERABILITY DATABASE, Information Technology Laboratory, [En línea]. (Recuperado en diciembre 2018.) Disponible en: https://nvd.nist.gov/

PACHECO, Ciro Alfonso. Análisis de seguridad del sistema de pedidos web de la empresa e.b. software Ltda. mediante pentesting. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2018, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://repository.unad.edu.co/bitstream/10596/21193/1/88285000.pdf

PLAZAS GARCIA, Edna Roció. Ingeniería social en las empresas colombianas. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2018, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

POSSO PAJARO Cristian & RIOS VERGARA Damián. Plan estratégico informático para la unidad
administrativa de la universidad de Cartagena. [En línea]. (Recuperado en octubre 2019.) Disponible en: http://190.242.62.234:8080/jspui/bitstream/11227/435/1/Plan%20Estrategico%20Informatico%20para%20la%20Unidad%20Administrativa%20de%20la%20Universidad%20de%20Cartagena.pdf

REYES ROSADO, Álvaro Rodrigo. Ataques en redes de datos IPv4 e IPv6. Tesis de Grado en Ingeniería Informática: Universidad de Málaga, 2016, [En línea]. (Recuperado en noviembre 2018.) Disponible en: http://hdl.handle.net/10630/13305

ORTIZ MANRIQUE, Edwin Omar. Análisis de causas de riesgos en la protección de la información de la empresa soltec-ing y recomendaciones de seguridad. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2018, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17448/1/13927687.pdf

SANCHEZ, Zulay. Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2017, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf

STOLK, Alejandra, Técnicas de Seguridad Informática con Software Libre, [En línea]. (Recuperado en noviembre 2018.) Disponible en: http://www.human.ula.ve/ceaa/temporal/fundamentos_de_seguridad.pdf

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (ITU), Las TICS y la sociedad, [En línea]. (Recuperado en octubre 2018.) Disponible en: https://www.itu.int/en/ITU-D/Digital-Inclusion/IndigenousPeoples/PublishingImages/Las%20TIC%20y%20la%20Sociedad.pdf

ZULUAGA MATEUS, Edna Rocio. Hacking ético basado en la metodología abierta de testeo de seguridad OSSTMM, aplicado a la rama judicial, seccional Armenia. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2017, [En línea]. (Recuperado en noviembre 2018.) Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

ANEXOS

ANEXO A. LISTADO DE VIDEOS

La ejecución practica de cada uno de los escenarios y sus correspondientes ataques informáticos se encuentra registrado en videos didácticos que le permiten al lector tener mayor compresión sobre las técnicas usadas para comprometer cada uno de los servidores. En la Tabla 9 se encuentran separados los videos por cada paso realizado y el video consolidado está disponible en https://youtu.be/hmPb8yeNUus.

Tabla 9. Listado de videos para el enfoque técnico

Titulo	**URL**
Presentación del laboratorio aplicado	https://youtu.be/AuhbKKXO40I
Escenario 1	
Escenario 1 punto A Actualización Kali Linux	https://youtu.be/JGZ2G49bHwo
Escenario 1 punto B Instalación de Metasploitable	https://youtu.be/IOta9PBm8r8
Escenario 1 punto C Escaneo de puertos con NMAP	https://youtu.be/TwH_L2qErDs
Escenario 1 punto D Ataque CGI PHP	https://youtu.be/F3tFGsbY9W0
Escenario 1 punto E Instalación de OpenVAS	https://youtu.be/lAH4165Njoc
Escenario 1 punto F Análisis con OpenVAS	https://youtu.be/RBJG-tu9zBM
Escenario 1 punto G Configuración Firewall IPTables	https://youtu.be/GS_nTYJ2FdI
Escenario 2	
Escenario 2 punto A Maquina Windows 7 vulnerable	https://youtu.be/fbYqbraJzH8
Escenario 2 punto B Escaneo de puertos con NMAP	https://youtu.be/TeMyh7BssiA
Escenario 2 punto C Análisis con OpenVAS	https://youtu.be/jatk71A7JMM
Escenario 2 punto D Ataque *EternalBlue*	https://youtu.be/i5cpqXTb0VE
Escenario 2 punto E *Payload Meterpreter*	https://youtu.be/4vlWimT02us
Escenario 2 punto F Actualización MS017 010	https://youtu.be/QPCXiq-7T84
Escenario 2 punto G Ingreso a la Deep Web	https://youtu.be/3euCg0o_j84

Fuente: El autor

ANEXO B. PROCEDIMIENTO DE RESPUESTA ANTE INCIDENTES

Un *Playbook* es el libro de jugadas, mejor conocido como procedimiento estándar de operación, que define las actividades a seguir por parte de organización para el manejo de un incidente informático y disminuir el tiempo de respuesta durante un ataque. El *playbook* de respuesta a incidentes contiene cuatro fases principales:

- Preparación.
- Detección y análisis.
- Contención, erradicación y recuperación.

- Post-incidente.

PLAYBOOK DEFACEMENT

En este *playbook* se describen las instrucciones prácticas para tratar un incidente relacionado con ataques de desfiguración en páginas web, la idea principal es garantizar la disponibilidad de los diferentes aplicativos definiendo medidas para restablecer el servicio, lo antes posible, a su estado normal. Adicionalmente, la finalidad es identificar patrones existentes de ataques web y bloquearlos de manera automática. En la Cuadro 23 están registradas las etapas y actividades que componen el procedimiento de respuesta y contención ante un incidente informático catalogado como *Defacemet*.

Cuadro 23. Playbook para un ataque de *Defacement*

Actividad		Descripción
Detección y Análisis	**Detección del Incidente**	Los ataques hacia las páginas web se detectan a través de las siguientes situaciones: • Elaborar la matriz de riesgos para todos los portales pertenecientes a la organización. • Tener un servidor web de respaldo donde pueda publicarse contenido durante el incidente. • Control Página Web: El contenido de la página web ha sido alterado. El nuevo contenido es o muy discreto o evidente. • Llamadas de usuarios o notificaciones por parte de los empleados acerca de problemas que notan durante la navegación por el sitio web. • Notificación realizada por el CSOC, donde se informa algún tipo de acción no autorizada o la detección de una alarma.
	Registrar e Identificar el incidente	El analista de seguridad informática recibe la notificación y registra el incidente. El analista de seguridad informática revisa la información del Incidente y su comportamiento. La información necesaria para determinar el impacto del incidente y tomar una acción es la siguiente: • Revisar los archivos con contenido estático, (fechas de modificación, firmas hash). • Comprobar enlaces de la página web (src, meta, css, script). • Validar la interfaz gráfica de la página web. • Analizar de manera cuidadosa y detallada el código fuente, (SAST y DAST). • FIM – (File Integrity Monitoring). • Cuál es el impacto del incidente y como afecta a la página web. • Definir el impacto inicial potencial. • Identificar la superficie del ataque.

Cuadro 23. (Continuación)

Actividad		Descripción
	Recolección de la información	Es importante tener recolección de información del portal web para determinar si el comportamiento ya se había detectado anteriormente. En general, se debe recolectar la siguiente información: • Logs del sistema, aplicación, red (Servidores, Equipos de Red, Dispositivos de seguridad). • Accesos al servidor web comprometido • Modificaciones del código fuente, FIM. • Transacciones de las bases de datos. • Correlación de eventos de seguridad. • Data volátil y validación de entradas de datos en el servidor.
Análisis	**Analizar datos recolectados**	Con la información recolectada se debe determinar si hay más activos afectados, lo que modificaría el Impacto potencial. Se debe determinar en este análisis: • Identificar el portal web comprometido o en riesgo. • Identifique cualquier código malicioso en el(los) sistema(s) afectado(s). • Identificar los medios y métodos utilizados por el presunto ciberdelincuente. • Validar operaciones maliciosas realizadas a nivel del aplicativo, sus componentes o en el servidor. • Averiguar el vector de ataque utilizado y corregir inmediatamente. • Servicios afectados de la compañía. • Validar si la vulnerabilidad explotada puede estar presente en otro activo que puede estar en riesgo.
	Seleccionar métodos de contención	Para mitigar las consecuencias generadas por el ataque hacia la página web, se deben realizar las siguientes acciones: • Respaldar todos los datos del servidor web, con fines forenses y recopilación de evidencia. • Si el origen del ataque es otro sistema de la red, desconéctelo si es físicamente posible e investíguelo. • Si el aplicativo web es crítico y no está disponible, se debe implementar un servidor web temporal donde se publique el mismo contenido o al menos un mensaje que indique "Temporalmente no disponible". Lo recomendable es mostrar contenido temporal estático. • Corregir la vulnerabilidad aplicando solución del fabricante. • Arreglar el fallo si se detecta una carpeta publica abierta o algún componente de terceros. • Modificación administrativa por acceso físico: modificar los derechos de acceso.
Contención/	**Evaluar el Impacto de la acción sobre la operación**	El ejecutor de la contención debe evaluar el impacto de aplicar el método seleccionado con base en el siguiente criterio: • ¿Se puede tener una afectación mayor si se ejecuta el método de contención? Si las acciones realizadas contuvieron el incidente, entonces se continua con la acción de contención. Si no, se debe consultar otros métodos de contención con el comité para la gestión de riesgos e incidentes.

Cuadro 23. (Continuación)

Actividad		Descripción
	Realizar acción de contención	Dependiendo el método de contención seleccionado, se aplican las acciones necesarias en la plataforma correspondiente. • Servidores, aplicaciones y Bases de Datos. • Componentes externos. • Framework o IDE, lenguaje de programación. • Motor de base de datos. • Equipos de Red o Seguridad
	Convocar Grupo de Respuesta ante Incidentes (GRI)	Se debe convocar a un comité del GRI, con el fin de tomar decisiones para la respuesta al incidente en los siguientes casos: • Las acciones de contención propuestas para detener el incidente no son viables debido a que pueden generar un impacto mayor sobre el servicio. • Las acciones aplicadas no contuvieron el incidente presentado.
	Revertir acciones realizadas	Eliminar todo el contenido alterado y sustituirlo por el contenido legítimo, restaurado de copias de seguridad previas. Garantizar que este contenido esté libre de vulnerabilidades. Si se ha usado un servidor respaldo, restaure el servidor web principal.
Post-Incidente	**Análisis de causa**	Se debe determinar la causa del Incidente: • Intencional o accidental. • Compromiso de una cuenta. • Maquina comprometida. • Bug del sistema. • Suplantación de la cuenta.
	Acciones de Cierre	Se debe documentar detalles del incidente, discutir las lecciones aprendidas, y ajustar los planes y las defensas. • Documentación del caso. • Notificación a los interesados. • Elaboración de informe. • Socializar el incidente. • Documentación de políticas.
Fuente: El autor, basado en la norma NIST 800-61 - Computer Security Incident Handling Guide.		

PLAYBOOK RANSOMWARE

En este *playbook* se describen las instrucciones prácticas para tratar un incidente relacionado con *ransomware*, la idea principal es dejar en cuarentena los dispositivos infectados lo antes posible para evitar que se propague el *ransowmare* en la red. Adicionalmente, la finalidad es identificar patrones existentes de

Ransowmare para bloquearlos de manera automática. En el Cuadro 24 están registradas las etapas y actividades que componen el procedimiento de respuesta y contención ante un incidente informático catalogado como *Ransomware*.

Cuadro 24. Playbook para un ataque de *Ransomware*

Actividad		Descripción
Detección y Análisis	**Detección del Incidente**	Una infección por ransomware se detecta a través de las siguientes situaciones: • Notificación del usuario final: El usuario afectado informa por correo electrónico o una llamada telefónica. • Notificación realizada por el CSOC, donde se informa la detección de comportamiento de tipo ransomware. • Detección por la solución antivirus End Point. • Antispam y otros filtros de correo electrónico.
	Registrar e Identificar el incidente	El analista de seguridad informática recibe la notificación y registra el incidente, acto seguido revisa la información del incidente y su comportamiento para determinar si se trata de un *ransomware* "*lockscreen"* o "*cryptolocker*". La información necesaria para determinar el impacto del incidente y tomar una acción es la siguiente: • Cuando la detección la realizo el usuario final, se debe establecer contacto y validar si se trata de un caso legítimo de ransomware. Algunas preguntas de rigor podrían ser: ¿A cuáles archivos o unidades no puede acceder?, ¿Aparece algún mensaje o archivo de texto con instrucciones?, ¿Las extensiones de los archivos han cambiado? • Cuando la detección la realizo el CSOC, se debe validar el patrón o IoC (Indicador de compromiso) y verificar la reputación en herramientas en línea. Si la alerta es genuina, se debe identificar el host impactado y notificar al usuario afectado que debe desconectar el dispositivo de la red. Posteriormente se debe recopilar información de la actividad reciente del usuario y enviar personal técnico para tomar una captura de la data volátil y llevar la maquina a cuarentena.
	Recolección de la información	En general, se debe recolectar la siguiente información para buscar IoC (Indicadores de compromiso), con base en el mismo patrón del host infectado: • Revisar URL desde los registros proxy y verifique la reputación. • Modificaciones en las rutas del sistema. • Correlación de eventos de seguridad, verificar la línea de tiempo de la maquina afectada y buscar eventos relacionados con detecciones de antivirus, logs del sistema, aplicación, red. • Realizar un volcado de la data volátil, memoria RAM, con la finalidad de realizar el análisis forense del incidente. • Registros de correo electrónico, filtros antispam. • Entrevista con el usuario final, validando si recibió un correo electrónico con un archivo adjunto en formato .zip, el cual al extraerse contiene archivos con extensión .vbs, .lnk o.swf, los cuales descargan la carga útil del ransomware, a través de un ejecutable o librería .dll.

Cuadro 24. (Continuación)

	Analizar datos recolectados	Con la información recolectada se debe determinar si hay más activos afectados, lo que modificaría el Impacto potencial. Se debe determinar en este análisis: • A partir del tráfico y registros de la víctima original, generar indicadores de compromiso con base en patrones potencialmente peligrosos. • Revisar vulnerabilidades que apuntan a versiones desactualizadas del navegador o del sistema operativo, por lo general versiones anteriores de Windows. Si los datos no son suficientes para determinar el impacto, se debe recolectar más información.
	Seleccionar métodos de contención	Lo importante es la acción oportuna e interrumpir la propagación del código malicioso usando los controles existentes: • Si fue un usuario quien detectó el incidente, se debe desconectar lo antes posible el equipo afectado y buscar en la red otros dispositivos que pueden estar comprometidos. • Si la detección fue generada por una alerta del SIEM, se debe identificar la estación de trabajo infectada y retirarla de la red para evitar propagación del ransomware. • Bloquear correos, servidores de correo y remitentes sospechosos, además se deben eliminar los correos maliciosos de las bandejas de entrada y advertir a los usuarios que no deben abrir enlaces o archivos adjuntos de dudosa procedencia. • Bloquear las URL maliciosas en el proxy e identificar que usuarios visitaron sitios web maliciosos. • Bloquear direcciones IP y dominios maliciosos en los equipos perimetrales. • Bloquear el acceso a las Herramientas de acceso remoto (RAT) identificadas para evitar comunicación con servidores de comando y control. • Suspender las credenciales de inicio de sesión de las cuentas sospechosas que han sido comprometidas. • Realizar un escaneo completo a las estaciones de trabajo. • Si el origen del ataque es otro sistema de la red, desconéctelo si es físicamente posible o envíelo a una VLAN de remediación. • Implementación de firmas personalizadas en la consola antivirus, para eliminar archivos o extensiones potencialmente peligrosos.
Contención/	**Evaluar el Impacto de la acción sobre la operación**	El ejecutor de la contención debe evaluar el impacto de aplicar el método seleccionado con base en el siguiente criterio: • ¿Se puede tener una afectación mayor si se ejecuta el método de contención? • ¿Se debe pagar el rescate? • ¿Es posible asumir la perdida de la información? Si las acciones realizadas contuvieron el incidente, entonces se continua con la acción de contención. Si no, se debe consultar otros métodos de contención con el comité para la gestión de riesgos e incidentes.

Cuadro 24. (Continuación)

	Realizar acción de contención	Dependiendo el método de contención seleccionado, se aplican las acciones necesarias en la plataforma correspondiente. • Servidores o estaciones de trabajo. • Aplicativos y componentes complementarios. • Equipos de Red o Seguridad. • Copias de seguridad y respaldo de sistemas.
	Convocar Grupo de Respuesta ante Incidentes (GRI)	Se debe convocar a un comité del GRI, con el fin de tomar decisiones para la respuesta al incidente en los siguientes casos: • Las acciones de contención propuestas para detener el incidente no son viables debido a que pueden generar un impacto mayor sobre el servicio. • Las acciones aplicadas no contuvieron el incidente presentado. • Informar a los propietarios de los datos y a las partes interesadas sobre el progreso de la contención.
	Erradicar y/o Revertir acciones realizadas	• Corregir la vulnerabilidad aplicando la solución del fabricante. • Limpiar la infección del equipo, usando una herramienta de seguridad endpoint o reinstalando el sistema. • Activar el proceso de eliminación automática o manual para erradicar el ransomware o ejecutables comprometidos usando las herramientas apropiadas. • Recuperar la información y los archivos mediante un respaldo limpio. • Volver a instalar cualquier sistema independiente desde una copia de seguridad limpia del sistema operativo antes de actualizar con copias de seguridad de datos confiables. • Realizar la restauración de los sistemas en red afectados desde una copia de seguridad confiable. • Continuar monitoreando las firmas y otros indicadores de compromiso para prevenir el resurgimiento del ataque. • Supervisar las estaciones de trabajo, en busca de algún archivo relacionado con el ransomware.
Post-Incidente	**Análisis de causa**	Se debe determinar la causa del Incidente: • Intencional o accidental. • Compromiso de una cuenta. • Maquina comprometida. • Bug del sistema. • Suplantación de la cuenta.
	Acciones de Cierre	Se debe documentar detalles del incidente, discutir las lecciones aprendidas, y ajustar los planes y las defensas. • Documentación del caso. • Notificación a los interesados. • Elaboración de informe. • Socializar el incidente. • Documentación de políticas.

Fuente: El autor, basado en la norma NIST 800-61 - Computer Security Incident Handling Guide.